QLOGIC

Simplify

SANbox 5602 Switch Management

User's Guide

Firmware Version 5.0

Information furnished in this manual is believed to be accurate and reliable. However, QLogic Corporation assumes no responsibility for its use, nor for any infringements of patents or other rights of third parties which may result from its use. QLogic Corporation reserves the right to change product specifications at any time without notice. Applications described in this document for any of these products are for illustrative purposes only. QLogic Corporation makes no representation nor warranty that such applications are suitable for the specified use without further testing or modification. QLogic Corporation assumes no responsibility for any errors that may appear in this document.

This product is covered by one or more of the following patents: 6697359; other patents pending.

QLogic, SANbox, SANsurfer, SANblade, SANsurfer Switch Manager, and SANsurfer Management Suite are trademarks or registered trademarks of QLogic Corporation.

Java and Solaris are registered trademarks of Sun Microsystems, Inc.

Gnome is a trademark of the GNOME Foundation Corporation.

Linux is a registered trademark of Linus Torvalds.

Mac OS X and Safari are registered trademarks of Apple Computer, Inc.

Microsoft, Windows NT, Windows 2000, Windows 2003, and Internet Explorer are trademarks of Microsoft Corporation.

Netscape Navigator and Mozilla are registered trademarks of Netscape Communications Corporation.

Red Hat is a registered trademark of Red Hat Software Inc.

All other brand and product names are trademarks or registered trademarks of their respective owners.

Document Revision History

Release, Revision A, February 2005

© 2000–2005 QLogic Corporation
First Printed: July 2004
All Rights Reserved Worldwide.
Printed in U.S.A.

Table of Contents

Section 1 Introduction

1.1 Intended Audience 1-1
1.2 Related Materials 1-1
1.3 JDOM License 1-1
1.4 Technical Support 1-2
1.4.1 Availability 1-3
1.4.2 Training 1-3
1.4.3 Contact Information 1-3

Section 2 Using SANsurfer Switch Manager

2.1 Workstation Requirements 2-2
2.2 Installing the Management Application 2-2
2.2.1 SANsurfer Switch Manager 2-3
2.2.2 SANsurfer Management Suite 2-4
2.2.2.1 SMS Installation for Windows 2-4
2.2.2.2 SMS Installation for Linux 2-6
2.2.2.3 SMS Installation for Solaris 2-8
2.3 Starting SANsurfer Switch Manager 2-10
2.4 Exiting SANsurfer Switch Manager 2-12
2.5 Uninstalling SANsurfer Switch Manager 2-13
2.5.1 SMS Uninstall 2-14
2.5.2 Standalone Uninstall 2-15
2.6 Changing the Encryption Key for the Default Fabric View File 2-15
2.7 Saving and Opening Fabric View Files 2-16
2.8 Setting SANsurfer Switch Manager Preferences 2-16
2.9 Using Online Help 2-18
2.10 Viewing Software Version and Copyright Information 2-18
2.11 SANsurfer Switch Manager User Interface 2-19
2.11.1 Menu Bars 2-20
2.11.1.1 Topology Display Menu 2-20
2.11.1.2 Faceplate Display Menu 2-21
2.11.1.3 Shortcut Keys 2-21
2.11.2 Tool Bar 2-22
2.11.3 Fabric Tree 2-23
2.11.4 Graphic Window 2-24
2.11.5 Data Window and Tabs 2-24

2.11.6 Working Status Indicator 2-24
2.12 Using the Topology Display 2-25
2.12.1 Switch and Link Status 2-25
2.12.2 Working with Switches and Links 2-26
2.12.2.1 Selecting Switches and Links 2-26
2.12.2.2 Arranging Switches in the Display 2-26
2.12.2.3 Opening the Faceplate and Topology Display Popup Menus 2-27
2.12.3 Topology Data Windows 2-27
2.13 Using the Faceplate Display 2-28
2.13.1 Port Views and Status 2-28
2.13.2 Working with Ports 2-29
2.13.2.1 Selecting Ports 2-29
2.13.2.2 Opening the Faceplate Popup Menu 2-29
2.13.3 Faceplate Data Windows 2-30

Section 3 Managing Fabrics

3.1 RADIUS Servers 3-1
3.1.1 Adding a RADIUS Server 3-2
3.1.2 Removing a RADIUS Server 3-4
3.1.3 Editing RADIUS Server Information 3-5
3.1.4 Modifying Authentication Order RADIUS Server Information 3-6
3.2 Securing a Fabric 3-7
3.2.1 Connection Security 3-7
3.2.2 User Account Security 3-8
3.2.3 Security Consistency Checklist 3-8
3.2.4 Device Security 3-9
3.2.4.1 Edit Security Dialog 3-10
3.2.4.2 Creating a Security Set 3-11
3.2.4.3 Create Security Group Dialog 3-12
3.2.4.4 Creating a Security Group 3-13
3.2.4.5 Create Security Group Member Dialog 3-14
3.2.4.6 Creating a Security Group Member 3-15
3.2.4.7 Editing the Security Configuration on a Switch 3-16
3.2.4.8 Viewing Properties of a Security Set, Group, or Member 3-17
3.2.4.9 Using the Security Config Dialog 3-17
3.2.4.10 Archiving a Security Configuration to a File 3-18
3.2.4.11 Activating a Security Set 3-18
3.2.4.12 Deactivating a Security Set 3-18
3.2.4.13 Configured Security Data Window 3-19
3.2.4.14 Active Security Data Window 3-19

3.2.5 Fabric Services ... 3-19
3.2.5.1 Enabling SNMP Configuration ... 3-20
3.2.5.2 Enabling In-band Management ... 3-20
3.3 Tracking Fabric Firmware and Software Versions ... 3-20
3.3.1 Saving a Version Snapshot ... 3-20
3.3.2 Viewing and Comparing Version Snapshots ... 3-21
3.3.3 Exporting Version Snapshots to a File ... 3-21
3.4 Managing the Fabric Database ... 3-22
3.4.1 Adding a Fabric ... 3-22
3.4.2 Removing a Fabric ... 3-23
3.4.3 Opening a Fabric View File ... 3-23
3.4.4 Saving a Fabric View File ... 3-24
3.4.5 Rediscovering a Fabric ... 3-24
3.4.6 Deleting Switches and Links ... 3-24
3.4.7 Adding a New Switch to a Fabric ... 3-25
3.4.8 Replacing a Failed Switch ... 3-26
3.5 Displaying Fabric Information ... 3-27
3.5.1 Fabric Status ... 3-27
3.5.2 Displaying the Event Browser ... 3-29
3.5.2.1 Filtering the Event Browser ... 3-31
3.5.2.2 Sorting the Event Browser ... 3-32
3.5.2.3 Saving the Event Browser to a File ... 3-32
3.5.3 Devices Data Window ... 3-33
3.5.4 Active Zone Set Data Window ... 3-34
3.5.4.1 Link Data Window ... 3-35
3.6 Working with Device Information and Nicknames ... 3-35
3.6.1 Displaying Detailed Device Information ... 3-35
3.6.2 Exporting Device Information to a File ... 3-36
3.6.3 Managing Device Port Nicknames ... 3-36
3.6.3.1 Creating a Nickname ... 3-36
3.6.3.2 Editing a Nickname ... 3-37
3.6.3.3 Deleting a Nickname ... 3-37
3.6.3.4 Exporting Nicknames to a File ... 3-37
3.6.3.5 Importing a Nicknames File ... 3-38
3.7 Zoning a Fabric ... 3-38
3.7.1 Zoning Concepts ... 3-38
3.7.1.1 Zones ... 3-39
3.7.1.2 Aliases ... 3-40
3.7.1.3 Zone Sets ... 3-40

3.7.1.4 Zoning Database ... 3-41
3.7.2 Using the Zoning Wizard ... 3-42
3.7.3 Managing the Zoning Database ... 3-42
3.7.3.1 Editing the Zoning Database ... 3-43
3.7.3.2 Configuring the Zoning Database ... 3-46
3.7.3.3 Saving the Zoning Database to a File ... 3-47
3.7.3.4 Restoring the Zoning Database from a File ... 3-47
3.7.3.5 Restoring the Default Zoning Database ... 3-48
3.7.3.6 Removing All Zoning Definitions ... 3-48
3.7.4 Managing Zone Sets ... 3-49
3.7.4.1 Creating a Zone Set ... 3-49
3.7.4.2 Activating and Deactivating a Zone Set ... 3-50
3.7.4.3 Copying a Zone to a Zone Set ... 3-50
3.7.4.4 Removing a Zone from a Zone Set or from All Zone Sets ... 3-51
3.7.4.5 Removing a Zone Set ... 3-51
3.7.5 Managing Zones ... 3-52
3.7.5.1 Creating a Zone in a Zone Set ... 3-53
3.7.5.2 Adding Zone Members ... 3-54
3.7.5.3 Renaming a Zone or a Zone Set ... 3-55
3.7.5.4 Removing a Zone Member ... 3-55
3.7.5.5 Removing a Zone from a Zone Set ... 3-55
3.7.5.6 Removing a Zone from All Zone Sets ... 3-55
3.7.5.7 Changing Zone Types ... 3-56
3.7.6 Managing Aliases ... 3-56
3.7.6.1 Creating an Alias ... 3-56
3.7.6.2 Adding a Member to an Alias ... 3-57
3.7.6.3 Removing an Alias from All Zones ... 3-57
3.7.7 Merging Fabrics and Zoning ... 3-58
3.7.7.1 Zone Merge Failure ... 3-58
3.7.7.2 Zone Merge Failure Recovery ... 3-58

Section 4 Managing Switches

4.1 Managing User Accounts ... 4-1
4.1.1 Creating User Accounts ... 4-3
4.1.2 Removing a User Account ... 4-4
4.1.3 Changing a User Account Password ... 4-5
4.1.4 Modifying a User Account ... 4-6
4.2 Displaying Switch Information ... 4-7
4.2.1 Devices Data Window ... 4-8
4.2.2 Switch Data Window ... 4-8

4.2.3 Port Statistics Data Window 4-12
4.2.4 Port Information Data Window 4-12
4.2.5 Configured Zonesets Data Window 4-13
4.3 Configuring Port Threshold Alarms 4-14
4.4 Paging a Switch 4-15
4.5 Setting the Date/Time and Enabling NTP Client 4-16
4.6 Resetting a Switch 4-16
4.7 Configuring a Switch 4-18
4.7.1 Using the Configuration Wizard 4-18
4.7.2 Switch Properties 4-19
4.7.2.1 Symbolic Name 4-19
4.7.2.2 Switch Administrative States 4-20
4.7.2.3 Domain ID and Domain ID Lock 4-21
4.7.2.4 Fabric Device Management Interface 4-21
4.7.2.5 Broadcast Support 4-22
4.7.2.6 In-band Management 4-22
4.7.3 Advanced Switch Properties 4-23
4.7.3.1 Interop Mode for Zoning 4-23
4.7.3.2 Legacy Port Address Format 4-24
4.7.3.3 Timeout Values 4-24
4.7.4 System Services Dialog 4-25
4.7.5 Security Consistency Checklist Dialog 4-26
4.7.6 Network Properties 4-27
4.7.6.1 IP Configuration 4-28
4.7.6.2 Remote Logging 4-29
4.7.6.3 NTP Client 4-29
4.7.7 SNMP Properties 4-30
4.7.7.1 SNMP Configuration 4-31
4.7.7.2 SNMP Trap Configuration 4-32
4.8 Managing Switch Stacks 4-33
4.8.1 Syslog 4-35
4.8.2 Select Source Dialog 4-35
4.9 Archiving a Switch 4-36
4.10 Restoring a Switch 4-37
4.11 Restoring the Factory Default Configuration 4-39
4.12 Downloading a Support File 4-41
4.13 Upgrading the Switch Using License Keys 4-41
4.14 Installing Firmware 4-42
4.14.1 Displaying Hardware Status 4-44

Section 5 Managing Ports

5.1 Displaying Port Information 5-1
5.1.1 Monitoring Port Status 5-2
5.1.1.1 Displaying Port Types 5-2
5.1.1.2 Displaying Port Operational States 5-3
5.1.1.3 Displaying Port Speeds 5-3
5.1.1.4 Displaying Transceiver Media Status 5-4
5.1.2 Port Statistics Data Window 5-5
5.1.3 Port Information Data Window 5-8
5.2 Configuring Ports 5-10
5.2.1 Changing Port Administrative States 5-11
5.2.2 Changing Port Speeds 5-12
5.2.3 Changing Port Types 5-13
5.2.4 I/O Stream Guard 5-13
5.2.5 Device Scan 5-14
5.2.6 Changing Port Symbolic Name 5-14
5.3 Using the Extended Credits Wizard 5-14
5.4 Resetting a Port 5-15
5.5 Testing Ports 5-16
5.6 Graphing Port Performance 5-18
5.6.1 Starting SANsurfer Performance Viewer 5-19
5.6.2 Exiting SANsurfer Performance Viewer 5-19
5.6.3 Saving and Opening Performance View Files 5-21
5.6.4 Changing the Default Performance View File Encryption Key 5-21
5.6.5 Setting SANsurfer Performance Viewer Preferences 5-22
5.6.6 Setting the Polling Frequency 5-22
5.6.7 Displaying Graphs for a Switch 5-23
5.6.7.1 Displaying Graphs for a Stack 5-23
5.6.7.2 Arranging Graphs in the Display 5-24
5.6.7.3 Customizing Graphs 5-24
5.6.7.4 Setting Global Graph Type 5-26
5.6.7.5 Rescaling a Selected Graph 5-26
5.6.8 Printing Graphs 5-26
5.6.9 Saving Graph Statistics to a File 5-26

Appendix A Command Line Interface

A.1 Logging On to a Switch A-1
A.2 User Accounts A-2
A.3 Working with Switch Configurations A-2

A.3.1 Modifying a Configuration A-3
A.3.2 Backing up and Restoring Switch Configurations A-4
A.4 Commands A-6
Admin Command A-8
Alias Command A-9
CIM Command A-11
CIMListener Command A-12
CIMSubscription Command A-14
Config Command A-16
Create Command A-19
Date Command A-22
Feature Command A-23
Firmware Install Command A-23
Group Command A-25
Hardreset Command A-33
Help Command A-34
History Command A-35
Hotreset Command A-36
Image Command A-37
Lip Command A-40
Passwd Command A-41
Ping Command A-42
Ps Command A-43
Quit Command A-44
Reset Command A-45
Security Command A-53
Securityset Command A-57
Set Command A-59
Set Config Command A-61
Set Log Command A-75
Set Port Command A-79
Set Setup Command A-81
Show Command A-91
Show Config Command A-106
Show Log Command A-109
Show Perf Command A-112
Show Setup Command A-114
Shutdown Command A-118
Test Command A-119

Uptime Command....A-122
User Command....A-123
Whoami Command....A-126
Zone Command....A-127
Zoneset Command....A-131
Zoning Command....A-133

Glossary

Index

Figures

Figure **Page**

2-1 Initial Startup Dialog....2-11
2-2 SANsurfer Switch Manager Window....2-12
2-3 Save Default Fabric View File Dialog....2-12
2-4 Load Default Fabric File Dialog....2-13
2-5 Preferences Dialog – SANsurfer Switch Manager....2-17
2-6 SANsurfer Switch Manager Display Elements....2-19
2-7 Topology Display Menu....2-20
2-8 Faceplate Display Menu....2-21
2-9 Fabric Tree....2-23
2-10 Topology Display....2-25
2-11 Faceplate Display....2-28
3-1 Add Radius Server....3-2
3-2 Remove Radius Server....3-4
3-3 Edit Radius Server Information....3-5
3-4 Modify Authentication Order - Radius Server Information....3-6
3-5 Edit Security Dialog....3-10
3-6 Create Security Group Dialog....3-12
3-7 Create a Security Group Member Dialog....3-14
3-8 Security Config Dialog....3-17
3-9 Fabric Version Snapshot Analysis Dialog....3-21
3-10 Add a New Fabric Dialog....3-22
3-11 Events Browser....3-29
3-12 Filter Events Dialog....3-31
3-13 Active Zone Set Data Window....3-34
3-14 Detailed Devices Display Dialog....3-35
3-15 Edit Zoning Dialog....3-43
3-16 Zoning Config Dialog....3-46
4-1 User Account Administration Dialog – Add Account....4-3
4-2 User Account Administration Dialog – Remove Account....4-4
4-3 User Account Administration Dialog – Change Password....4-5
4-4 User Account Administration Dialog - Modify Account....4-6

4-5 Faceplate Display - Switch Information 4-7
4-6 Configured Zonesets Data Window 4-13
4-7 Port Threshold Alarm Configuration Dialog 4-14
4-8 Port Threshold Alarm Example 4-15
4-9 Switch Properties Dialog 4-19
4-10 Advanced Switch Properties Dialog 4-23
4-11 System Services Dialog 4-25
4-12 Network Properties Dialog 4-27
4-13 SNMP Properties Dialog 4-30
4-14 Switch Stacks 4-33
4-15 Syslog Dialog 4-35
4-16 Restore Dialogs – Full and Selective 4-37
4-17 Features License Key Dialog 4-42
4-18 Add License Key Dialog 4-42
4-19 Hardware Status LEDs 4-44
5-1 Faceplate Display – Port Information 5-1
5-2 Port Properties Dialog 5-10
5-3 Designate Donor Ports 5-15
5-4 Port Loopback Test Dialog 5-16
5-5 Fabric View Graphs 5-18
5-6 Save Default Performance View File Dialog 5-20
5-7 Load Default View File Dialog 5-20
5-8 Preferences – SANsurfer Performance Viewer 5-22
5-9 Default Graph Options Dialog 5-24

Tables

Table **Page**

2-1 Workstation Requirements 2-2
2-2 Tool Bar Buttons 2-22
3-1 Topology Display Switch and Status Icons 3-28
3-2 Severity Levels 3-30
3-3 Devices Data Window Entries 3-33
3-4 Edit Zoning Dialog Tool Bar Buttons and Icons 3-45
4-1 Factory User Accounts 4-2
4-2 Switch Data Window Entries 4-8
4-3 Switch Resets 4-17
4-4 Switch Administrative States 4-20
4-5 Timeout Values 4-24
4-6 IP Configuration Parameters 4-28
4-7 SNMP Configuration Parameters 4-31
4-8 SNMP Trap Configuration Parameters 4-32
4-9 Factory Default Configuration Settings 4-39
5-1 Port Types 5-2
5-2 Port Operational States 5-3
5-3 Port Speeds 5-3

5-4 Port Transceiver Media View 5-4
5-5 Port Statistics Data Window Entries 5-5
5-6 Port Information Data Window Entries 5-8
5-7 Port Administrative States 5-11
5-8 Port Speeds 5-12
5-9 Port Types 5-13
A-1 Command-Line Completion A-6
A-2 Commands Listed by Authority Level A-7
A-3 CIM Listener Configuration Parameters A-12
A-4 CIM Subscription Configuration Parameters A-14
A-5 ISL Group Member Attributes A-26
A-6 Port Group Member Attributes A-27
A-7 MS Group Member Attributes A-28
A-8 Group Member Attributes A-29
A-9 Switch Configuration Defaults A-47
A-10 Port Configuration Defaults A-48
A-11 Port Threshold Alarm Configuration Defaults A-49
A-12 Zoning Configuration Defaults A-49
A-13 SNMP Configuration Defaults A-50
A-14 RADIUS Configuration Defaults A-50
A-15 Services Configuration Defaults A-51
A-16 System Configuration Defaults A-52
A-17 Security Configuration Defaults A-52
A-18 Set Config Port Parameters A-61
A-19 Security Configuration Parameters A-64
A-20 Set Config Switch Parameters A-65
A-21 Set Config Threshold Parameters A-67
A-22 Set Config Zoning Parameters A-68
A-23 RADIUS Service Settings A-81
A-24 Switch Services Settings A-83
A-25 SNMP Configuration Settings A-85
A-26 System Configuration Settings A-86
A-27 Show Port Parameters A-94
A-28 Switch Operational Parameters A-97
A-29 Zoning Database Limits A-134

Section 1
Introduction

This manual describes the switch management tools which include the SANsurfer Switch Manager application (version 5.00) and the Command Line Interface (CLI) for the SANbox 5602 Fibre Channel switch (firmware version 5.0). The SANbox 5602 switch is a 20-port non-blocking Fibre Channel switch. This manual defines the features, components, and performance characteristics of the SANbox 5602 switch. The SANsurfer Switch Manager application is the primary focus of this manual which is organized as follows:

- Section 1 describes the intended audience for this manual, related materials, and technical support.
- Section 2 describes how to use SANsurfer Switch Manager, its menus, and its displays.
- Section 3 describes fabric management tasks.
- Section 4 describes switch management tasks.
- Section 5 describes port and device management tasks.
- Appendix A describes the command line interface.

A glossary of terms and an index are also provided.

1.1 Intended Audience

This manual introduces the switch management products and explains their installation and use. It is intended for users responsible for installing and using switch management tools.

1.2 Related Materials

Refer to the following manuals for information about switch hardware and installation.

- *SANbox 5602 Fibre Channel Switch Installation Guide*, publication number 59096-01 Rev. A.

1.3 JDOM License

This product includes software developed by the JDOM Project (http://www.jdom.org/). Copyright (C) 2000-2002 Brett McLaughlin & Jason Hunter. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions, and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the disclaimer that follows these conditions in the documentation and/or other materials provided with the distribution.
3. The name "JDOM" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact license@jdom.org.
4. Products derived from this software may not be called "JDOM", nor may "JDOM" appear in their name, without prior written permission from the JDOM Project Management (pm@jdom.org).

In addition, we request (but do not require) that you include in the end-user documentation provided with the redistribution and/or in the software itself an acknowledgement equivalent to the following: "This product includes software developed by the JDOM Project (http://www.jdom.org/)."

Alternatively, the acknowledgment may be graphical using the logos available at http://www.jdom.org/images/logos.

THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE JDOM AUTHORS OR THE PROJECT CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This software consists of voluntary contributions made by many individuals on behalf of the JDOM Project and was originally created by Brett McLaughlin <brett@jdom.org> and Jason Hunter <jhunter@jdom.org>. For more information on the JDOM Project, please see <http://www.jdom.org/>.

1.4 Technical Support

Customers should contact their authorized maintenance provider for technical support of their QLogic switch products. QLogic-direct customers may contact QLogic Technical Support; others will be redirected to their authorized maintenance provider.

Visit the QLogic support Web site listed in Contact Information for the latest firmware and software updates.

1.4.1 Availability

QLogic Technical Support is available from 7:00 AM to 7:00 PM Central Standard Time, Monday through Friday, excluding QLogic-observed holidays.

1.4.2 Training

QLogic offers certification training for the technical professional for both the SANblade™ HBAs and the SANbox 5602 switches. From the training link at www.qlogic.com, you may choose Electronic-Based Training or schedule an intensive "hands-on" Certification course.

Technical Certification courses include installation, maintenance and troubleshooting QLogic SAN products. Upon demonstrating knowledge using live equipment, QLogic awards a certificate identifying the student as a Certified Professional. The training professionals at QLogic may be reached by email at tech.training@qlogic.com

1.4.3 Contact Information

Telephone:	+1 952-932-4040
Fax:	+1 952-932-4018
Email:	
Technical Service	support@qlogic.com
Technical Training	tech.training@qlogic.com
QLogic Web Site:	www.qlogic.com
Technical Support Web Site:	support.qlogic.com

Notes

Section 2

Using SANsurfer Switch Manager

This section describes how to use the SANsurfer Switch Manager application and its menus. The following topics are covered:

- Workstation Requirements
- Installing the Management Application
- Starting SANsurfer Switch Manager
- Exiting SANsurfer Switch Manager
- Uninstalling SANsurfer Switch Manager
- Changing the Encryption Key for the Default Fabric View File
- Saving and Opening Fabric View Files
- Setting SANsurfer Switch Manager Preferences
- Using Online Help
- Viewing Software Version and Copyright Information
- SANsurfer Switch Manager User Interface
- Using the Topology Display
- Using the Faceplate Display

2.1 Workstation Requirements

The requirements for fabric management workstations running SANsurfer Switch Manager are described in Table 2-1:

Table 2-1. Workstation Requirements

Operating System	■ Windows® 2000, 2003, and XP ■ Solaris™ 8, 9, and 10 ■ Linux® Red Hat® EL 3.x ■ S.u.S.E® Linux 9.0 Enterprise ■ Mac OS X® 10.3
Memory	256 MB or more
Disk Space	150 MB per installation
Processor	500 MHz or faster
Hardware	CD-ROM drive, RJ-45 Ethernet port, RS-232 serial port (optional)
Internet Browser	Microsoft® Internet Explorer® 5.0 and later Netscape® Navigator® 4.72 and later Mozilla™ 1.02 and later Safari® Java 2 Run Time Environment to support the web applet

Telnet workstations require an RJ-45 Ethernet port or an RS-232 serial port and an operating system with a Telnet client.

2.2 Installing the Management Application

You can manage the switch using SANsurfer Switch Manager as a standalone application or as a part of SANsurfer Management Suite™. SANsurfer Management Suite is QLogic's integrated fabric management application, managing both HBAs and switches.

- If your switch was shipped with a SANsurfer Switch Manager Disk, refer to "SANsurfer Switch Manager" on page 2-3 for instructions on how to install SANsurfer Switch Manager.
- If your switch was shipped with a SANsurfer Management Suite Disk, refer to "SANsurfer Management Suite" on page 2-4 for instructions on how to install and upgrade SANsurfer Management Suite.

2.2.1 SANsurfer Switch Manager

You can install SANsurfer Switch Manager on a Windows, Linux, Solaris, or Mac OS X workstation. To install the SANsurfer Switch Manager application from the SANsurfer Switch Manager Installation Disk, do the following:

For a Windows platform:

1. Close all programs currently running, and insert the SANsurfer Switch Manager Installation Disk into the management workstation CD-ROM drive.
2. In the upper left corner of the product introduction screen, click **Management Software**.
3. Locate your platform in the table and click **Install**.

If the product introduction screen does not open in step 2, open the CD with Windows Explorer and run the installation program with the following path:

```
data\files\Management_Software\Windows\Windows_5.00.xx.xx.exe
```

For a Linux platform:

Open the CD and run the installation program with the following path:

```
data/files/Management_Software/Linux/Linux_5.00.xx.xx.bin
```

If there is no CD-ROM icon, do the following:

1. Open an xterm or other terminal window.
2. Mount the CD-ROM. From a shell prompt, enter the following:

   ```
   mount /mnt/cdrom
   ```
3. Change directory to the location of the install program:

   ```
   cd /mnt/cdrom/data/files/Management_Software/Linux
   ```
4. Execute the install program and follow the installation instructions.

   ```
   Linux_5.00.xx.xx.bin
   ```

For a Solaris platform:

1. Open a terminal window. If the disk isn't already mounted, enter the following command:

   ```
   volcheck
   ```
2. Enter following command to move to the directory on the CD that contains the executable:

   ```
   cd /cdrom/cdrom0/data/files/Management_Software/solaris
   ```
3. Execute the install program and follow the installation instructions:

   ```
   Solaris_5.00.xx.xx.bin
   ```

For a Mac OS X platform:

1. Open the CD and move to the following folder:

   ```
   data/files/Management_Software/MacOSX
   ```

2. Double click the applicaton zip file (MacOSX_5.00.xx_xxxx.zip). This will place the install program on your desktop.
3. Locate the **Install** program icon on your desktop, execute it, and follow the installation instructions.

2.2.2 SANsurfer Management Suite

The following instructions describe how to install SANsurfer Management Suite and upgrade SANsurfer Switch Manager. You can install SANsurfer Management Suite (SMS) on a Windows, Linux, or Solaris workstation. Choose the instructions for your workstation:

- SMS Installation for Windows
- SMS Installation for Linux
- SMS Installation for Solaris

2.2.2.1 SMS Installation for Windows

Close all programs currently running, and insert the SANsurfer Management Suite Installation Disk into the management workstation CD-ROM drive.

1. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Using Windows Explorer, double-click the drive letter which contains the SANsurfer Management Suite Disk.
   b. Locate and double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox 5602 Series area.
4. In the Operating System column, click the **Win NT/2000** link.
5. Click the **SANsurfer Management Software** link to open the File Download dialog.

6. You can run the installation file from the CD-ROM or download the installation file to your hard drive. Choose one of the following:
   - Open the installation file from the CD-ROM and follow the SANsurfer Switch Manager installation instructions.
   - Specify a location in which to save the **sansurfer_windows_install.exe** file, and click the **Save** button. Double-click the saved **sansurfer_windows_install.exe** file and follow the installation instructions.
7. When the installation is complete, start SANsurfer Management Suite using the SANsurfer file from the SANsurfer Management Suite installation directory. You can also start SANsurfer Management Suite by clicking the SANsurfer icon (if installed) on the desktop or from the Start menu. In SMS, Click the **Switch** tab in the left pane. From the Help menu, select **About ...** and make note of the version number. Close SANsurfer Management Suite.
8. To ensure you are using the most recent version of SANsurfer Switch Manager, visit the QLogic support web page and go to Drivers, Software and Manuals.
   a. Select your switch model from the pull-down menu. Locate the description for SANsurfer Switch Manager for Windows under "Management Software".
   b. If the release version number (5.00.xx) is greater than what is currently installed, download the new version and proceed to step 9. Otherwise, no upgrade is needed and the SMS installation is complete.
9. To start the installer, open the zip file and run the **SANsurferSwitchMgr_Windows_5.00.xx.exe** file.
10. When prompted for an installation directory, click the **Choose** button and select the same folder as the SANsurfer Management Suite installation in step 6. The default SMS installation directory is **C:\Program Files\QLogic Corporation\SANsurfer**. Click the Next button.
11. When prompted for the location in which to create the program icons, click the **In an Existing Group** radio button, then specify the same group that was used for the SMS installation. The default SMS group is "QLogic Management Suite". Click the **Next** button.
12. Click the **Install** button to the start the installation. When the installation is complete, click the **Done** button.
13. In the SMS install directory, enter the following command to execute the chglax.bat file. If prompted to overwrite an existing file, enter `Y` to do so.

    ```
    chglax.bat
    ```

14. Restart SANsurfer Switch Manager from SANsurfer Management suite as you did in step 7 and confirm that the new version is running.

2.2.2.2
SMS Installation for Linux

Close all programs currently running, and insert the SANsurfer Management Suite Installation Disk into the management workstation CD-ROM drive.

1. If a file browser dialog opens showing icons for the contents of the CD-ROM, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page. If a file browser does not open, double-click the CD-ROM icon to open the browser. If there is no CD-ROM icon, do the following:
   a. Open an xterm or other terminal window.
   b. Mount the CD-ROM. From a shell prompt, enter the following command:

      ```
      mount /mnt/cdrom
      ```

   c. Execute your web browser to view the **Start_Here.htm** document using one of the following commands:

      ```
      mozilla file:/mnt/cdrom/Start_Here.htm
      ```

      or

      ```
      netscape file:/mnt/cdrom/Start_Here.htm
      ```

   d. The SANsurfer Management Suite start page opens in your browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox 5602 Series area.
4. In the Operating System column, click the **Linux** link.
5. Click the **SANsurfer Management Software** link to open the File Download dialog.
6. Enter a path name to save the **sansurfer_linux_install.bin** file, and click the **Save** button.
7. Open a terminal window for the directory in which the **sansurfer_linux_install.bin** file was saved, and make the file executable.

   ```
   chmod +x sansurfer_linux_install.bin
   ```

8. Execute the install program and follow the installation instructions

   ```
   ./sansurfer_linux_install.bin
   ```

9. When the installation is complete, start SANsurfer Management Suite using the SANsurfer file in the installation directory. Click the **Switch** tab from the left pane to open SANsurfer Switch Manager. From the Help menu, select **About ...** and make note of the release version number. Close SANsurfer Management Suite.

10. To ensure that you are using the most recent version of SANsurfer Switch Manager, visit the QLogic support web page and go to Drivers, Software and Manuals.
    a. Select your switch model from the pull-down menu. Locate the description for SANsurfer Switch Manager for Linux under "Management Software".
    b. If the release version number (5.00.xx) is greater than what is currently installed on your workstation, down load the new version and proceed to step 11. Otherwise, no upgrade is needed and the SMS installation is complete.
11. From the tar.gz file, extract the **SANsurferSwitchMgr_Linux_5.00.xx.bin** file and make the file executable.

    ```
    chmod +x sansurferswitchmgr_linux_5.02.xx.bin
    ```

12. Execute the install program and follow the installation instructions.

    ```
    ./sansurferswitchmgr_linux_5.02.xx.bin
    ```

13. When prompted for an installation directory, click the **Choose** button and select the same folder as the SANsurfer Management Suite installation in step 9. The default SMS installation directory is /opt/QLogic_Corporation/SANsurfer.
14. Enter the following script command from the installation directory:

    ```
    ./chglax
    ```

15. Start SANsurfer Switch Manager from SANsurfer Management suite as you did in step 9 and confirm that the new version is running.

2.2.2.3

SMS Installation for Solaris

To install the SANsurfer Switch Manager application on Solaris from the SANsurfer Management Suite CD-ROM, do the following:

1. Insert the SANsurfer Management Suite Disk into the management workstation CD-ROM drive. If the SANsurfer Management Suite start page does not open in your default browser, do the following:
   a. Right-click the Workspace Menu.
   b. Select **File**, then select **File Manager**.
   c. In File Manager, double-click the CD-ROM folder, and then double-click the Sansurfer folder.
   d. In the Sansurfer folder, double-click the **Start_Here.htm** file to open the SANsurfer Management Suite start page in your default browser.
2. On the SANsurfer Management Suite start page, click the **SANbox Switch Software** button.
3. On the SANbox Switch Software page, scroll to the SANbox 5602 Series area.
4. In the Operating System column, click the **Solaris SPARC** link.
5. Click the **SANsurfer Management Software** link to open the Save As dialog.
6. Enter a path name to save the **sansurfer_solaris_install.bin** file and click the **Save** button.
7. Open a terminal window for the directory in which the **sansurfer_solaris_install.bin** file was saved, and enter the following:

   ```
   chmod +x sansurfer_solaris_install.bin
   ```

8. Execute the install program and follow the installation instructions:

   ```
   ./sansurfer_solaris_install.bin
   ```

9. When the installation is complete, start SANsurfer Management Suite using the SANsurfer file in the installation directory. Click the **Switch** tab from the left pane to open SANsurfer Switch Manager. From the Help menu, select **About ...** and make note of the release version number. Close SANsurfer Management Suite.
10. To ensure that you are using the most recent version of SANsurfer Switch Manager, visit the QLogic support web page and go to Drivers, Software and Manuals.
    a. Select your switch model from the pull-down menu. Locate the description for SANsurfer Switch Manager for Linux under "Management Software".

b. If the release version number (5.00.xx) is greater than what is currently installed on your workstation, down load the new version. Otherwise, no upgrade is needed.

11. Open the tar file and save the **SANsurferSwitchMgr_QLGCsol_5.00.xx.bin** file in a folder and make the file executable.

```
# chmod +x sansurferswitchmgr_QLGCsol_5.00.xx
```

12. Install the new SANsurfer Switch Manager package:

```
# pkgadd -d sansurferswitchmgr_QLGCsol_5.00.xx
```

13. Change directories to the package location:

```
# cd /usr/opt/QLGCsol/bin
```

14. Locate and execute the file **sbm_over_sms.sh**:

```
# ./sbm_over_sms.sh
```

15. When prompted for the SMS installation directory, enter **d** if SMS was installed in it's default directory (/opt/QLogic_Corporation/SANsurfer). Otherwise, enter the path name for the SMS installation directory. The script will copy the necessary files to the specified installation directory.

16. Restart SANsurfer Switch Manager from SANsurfer Management suite as you did in step 9 and confirm that the new version is running.

2.3 Starting SANsurfer Switch Manager

You can start SANsurfer Switch Manager as a standalone application or from SANsurfer Management Suite.

Note: After the switch is operational, you can also open the SANsurfer Switch Manager web applet, by entering the switch IP address in an internet browser. If your workstation does not have the Java 2 Run Time Environment program, you will be prompted to download it.

- To start SANsurfer Switch Manager as a standalone application, do the following.
  1. Start the SANsurfer Switch Manager using one of the following methods:
     - For Windows, double-click the SANsurfer Switch Manager shortcut, or select SANsurfer Switch Manager from Start menu, depending on how you installed the SANsurfer Switch Manager application. From a command line, you can enter the SANsurfer_Switch_Manager command:

       ```
       <install_directory>SANsurfer_Switch_Manager.exe
       ```

     - For Linux, Solaris, or Mac OS X, enter the SANsurfer_Switch_Manager command:

       ```
       <install_directory>./SANsurfer_Switch_Manager
       ```

  2. In the Initial Start dialog, click the **Open Configuration Wizard** button. When you power up the switch, the Configuration Wizard will recognize the switch and lead you through the configuration process.
- To start SANsurfer Switch Manager from SANsurfer Management Suite, do the following.
  1. Start the SANsurfer Management Suite application using one of the following methods:
     - For Windows, double-click the SANsurfer shortcut, or select **SANsurfer** from Start menu, depending on how you installed the SANsurfer application. From a command line, enter the following command:

       ```
       <install_directory>\SANsurfer.exe
       ```

     - For Linux or Solaris enter the SANsurfer command:

       ```
       <install_directory>./SANsurfer
       ```

  2. From the SANsurfer Management Suite home page, click the SANsurfer Switch Manager button.

3. In the Initial Start dialog, click the **Open Configuration Wizard** button. When you power up the switch, the Configuration Wizard will recognize the switch and lead you through the configuration process.

The application opens with the Initial Start dialog shown in Figure 2-1. If you prefer not to see this dialog, check the **Don't show this dialog again** box. This has the same effect as disabling the Display Initial Startup Dialog preference. Refer to "Setting SANsurfer Switch Manager Preferences" on page 2-16 for information about setting preferences.

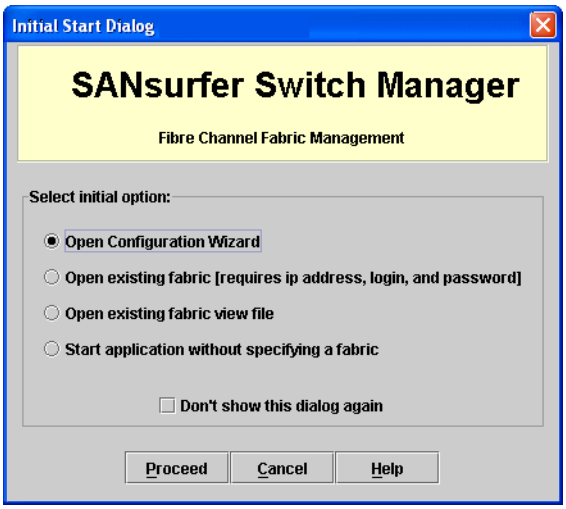


Figure 2-1. Initial Startup Dialog

- Click the **Open Existing Fabric** radio button to open the Add a New Fabric dialog, which prompts you for a fabric name, IP address, account name, and password. Refer to "Adding a Fabric" on page 3-22.
- Click the **Open Existing Fabric View File** radio button to open the Open View dialog which prompts you to specify a fabric view file that you saved earlier. Refer to "Opening a Fabric View File" on page 3-23.

- Click the **Start Application Without Specifying a Fabric** radio button to open the SANsurfer Switch Manager window shown in Figure 2-2.
- Click the **Open Configuration Wizard** radio button to open the Config Wizard to configure a switch, add a new switch, replace/restore a switch, or recover or edit an IP configuration of an existing switch.

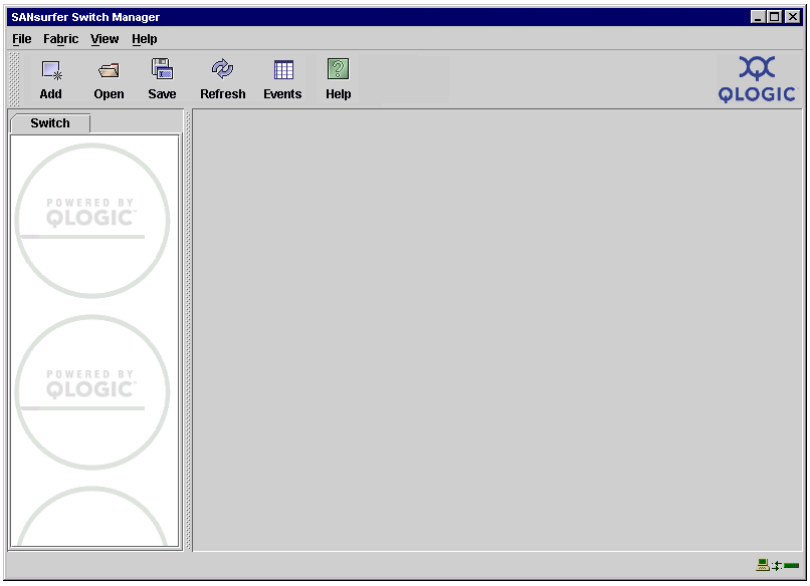


Figure 2-2. SANsurfer Switch Manager Window

2.4 Exiting SANsurfer Switch Manager

To exit a SANsurfer Switch Manager application session, open the File menu and select **Exit**. If you have not yet defined an encryption key, the Save Default Fabric View File dialog, shown in Figure 2-3, prompts you to save the current fabric view as the default fabric view file. Enter an encryption key in the Default Fabric File Encryption Key field. Re-enter the encryption key in the Re-enter Encryption Key to Confirm field. Click the **OK** button to save the current set of fabrics to the default fabric view file in the working directory.

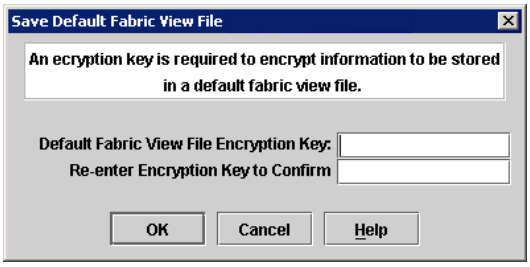

Save Default Fabric View File
An ecryption key is required to encrypt information to be stored in a default fabric view file.
Default Fabric View File Encryption Key:
Re-enter Encryption Key to Confirm
OK
Cancel
Help

Figure 2-3. Save Default Fabric View File Dialog

The encryption key is used to encrypt the sensitive data in the default fabric view file. Refer to ”Changing the Encryption Key for the Default Fabric View File” on page 2-15 for information about changing this encryption key. If an encryption key has been defined and the View File Auto Save and Load preferences settings are set to Enable, the current fabric view is automatically saved to your default fabric view file upon exit future SANsurfer Switch Manager sessions.

To prevent SANsurfer Switch Manager from prompting you to save the default fabric view file between SANsurfer Switch Manager sessions, set the View File Auto Save and Load preferences setting to Enable (default). Refer to ”Setting SANsurfer Switch Manager Preferences” on page 2-16 for more information.

In your next SANsurfer Switch Manager session, the Load Default Fabric File dialog shown in Figure 2-4 prompts you to load the default fabric view file and to specify its encryption key, if there is one. In the Default Fabric File Encryption Key field, enter the encryption key and click the **Load View File** button. If you do not want to load the default fabric view file, click the **Continue Without Loading** button to open the SANsurfer Switch Manager with no fabric displayed.

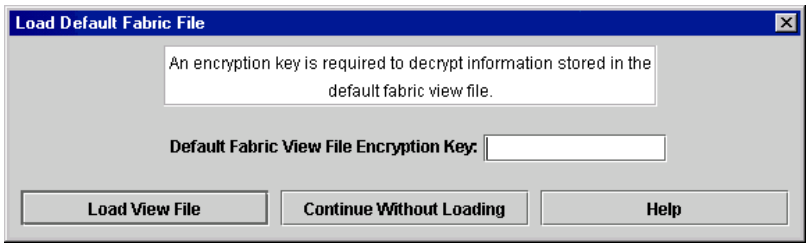

Load Default Fabric File
An encryption key is required to decrypt information stored in the default fabric view file.
Default Fabric View File Encryption Key:
Load View File
Continue Without Loading
Help

Figure 2-4. Load Default Fabric File Dialog

2.5 Uninstalling SANsurfer Switch Manager

The method you use to uninstall SANsurfer Switch Manager depends on how you installed it:

- If you installed SANsurfer Switch Manager as part of SANsurfer Management Suite, you must uninstall SANsurfer Management Suite. Refer to ”SMS Uninstall” on page 2-14.
- If you installed SANsurfer Switch Manager as a standalone program, you must uninstall SANsurfer Switch Manager directly. Refer to ”Standalone Uninstall” on page 2-15.

2.5.1
SMS Uninstall

A program to uninstall SANsurfer Management Suite was included as part of the SANsurfer Management Suite installation process. Use this method only if you installed SANsurfer Switch Manager as part of SANsurfer Management Suite. The UninstallData folder in the installation directory contains the uninstall program, SANsurferUninstaller.

The default installation directories are:

- For Windows: C:\Program Files\QLogic_Corporation\SANsurfer
- For Linux: /opt/QLogic_Corporation/SANsurfer
- For Solaris: /opt/QLogic_Corporation/SANsurfer

To uninstall the SANsurfer Management Suite application, do the following:

- For Windows, browse for the uninstall program file or the shortcut/link that points to the uninstall program file. The uninstall program shortcut is in the same folder as the program shortcut (Start menu, program group, on desktop, or user specified) that is used to start the SANsurfer Management Suite application. Double-click the uninstall program file or shortcut/link, and follow the instructions.
- For Linux, execute the link to SANsurferUninstaller.

  ```
  <install_directory>/UninstallerData/SANsurferUninstaller
  ```

- For Solaris, enter the following command and follow the instructions:

  ```
  <install_directory>/UninstallData/SANsurferUninstaller
  ```

2.5.2 Standalone Uninstall

A program to uninstall SANsurfer Switch Manager was included as part of the installation process. Use this method only if you installed SANsurfer Switch Manager as a standalone program. The UninstallerData folder in the Install directory contains the uninstall program, Uninstall_SANsurfer_Switch_Manager. Also, a shortcut/link to the uninstall program was installed in the installation directory during the SANsurfer Switch Manager installation process.

The default installation directories are:

- For Windows: C:\Program Files\QLogic_Corporation\SANsurfer_Switch_Manager
- For Linux: /opt/QLogic_Corporation/SANsurfer_Switch_Manager
- For Solaris: /usr/opt/QLogic_Corporation/SANsurfer_Switch_Manager
- For Mac OS X: Users/qlogic/Applications/QLogic_Corporation/SANsurfer_Switch_Manager

To uninstall the SANsurfer Switch Manager application, do the following:

- For Windows, browse for the uninstall program file or the shortcut/link that points to the uninstall program file. The uninstall program shortcut is in the same folder as the program shortcut (Start menu, program group, on desktop, or user specified) that is used to start the SANsurfer Switch Manager application. Double-click the uninstall program file or shortcut/link, and follow the instructions to uninstall the SANsurfer Switch Manager application.
- For Linux, Solaris, or Mac OS X, execute the link to Uninstall_SANsurfer_Switch_Manager. If no links were created during the installation, enter the Uninstall_SANsurfer_Switch_Manager command from the following directory:

  ```
  UninstallerData/Uninstall_SANsurfer_Switch_Manager
  ```

2.6 Changing the Encryption Key for the Default Fabric View File

To change the encryption key for the SANsurfer Switch Manager default fabric view file, do the following:

1. Open the File menu and select **Save Default Fabric View File** to open the Save Default Fabric View File dialog. Enter an encryption key in the Default Fabric File Encryption Key field.
2. Re-enter the same encryption key in the Re-enter Encryption Key to Confirm field.
3. Click the **OK** button to save the current set of fabrics to the default fabric view file in the working directory.

2.7 Saving and Opening Fabric View Files

A fabric view file is one or more fabrics saved to a file. In addition to the SANsurfer Switch Manager default fabric view file, you can save and open your own fabric view files. To save a set of fabrics to a file, do the following:

1. Open the File menu and select **Save View As** to open the Save View dialog.
2. Enter a name for the fabric view file or click the **Browse** button to select an existing file. Files are saved in the working directory.
3. Enter a password. When you attempt to open this fabric view file, you will be prompted for this password. If you leave the File Password field blank, no password will be required when attempting to open this fabric view file.
4. Click the **OK** button to save the view.

To open a fabric view file, do the following:

1. Open the File menu and select **Open View File** to open the Open View dialog.
2. Enter a name for the fabric view file or click the **Browse** button to select an existing file.
3. If the fabric view file was saved with a password, enter the password and click the **OK** button.
4. Click the **OK** button to open the view.

2.8 Setting SANsurfer Switch Manager Preferences

Using the preferences settings, you can:

- Change the location of the working directory in which to save files.
- Change the location of the browser used to view the online help. The Browser Location field is not supported/displayed for Macintosh OS X.
- Choose the fabric discovery interval. The fabric discovery interval is how often the SANsurfer Switch Manager application receives information from the fabric. Choose 30 (default), 45, or 60 seconds. The smaller the interval, the more often the application talks to the switch and thus the greater impact to performance.
- Enable (default) or disable the view file auto save and load feature. Refer to ”Exiting SANsurfer Switch Manager” on page 2-12 for more information on the default fabric view file.
- Enable (default) or disable the use of the Initial Start Dialog at the beginning of a SANsurfer Switch Manager session. Refer to ”Starting SANsurfer Switch Manager” on page 2-10 for information about the Initial Start Dialog. After a default fabric view file is created, this setting has no effect.

- Enable (default) or disable the Event Browser. Refer to ”Displaying the Event Browser” on page 3-29. If the Event Browser is enabled using the Preferences dialog as shown in Figure 2-5, the next time SANsurfer Switch Manager is started, all events will be displayed. If the Event Browser is disabled when SANsurfer Switch Manager is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.
- Choose the default port view when opening the faceplate display. You can set the faceplate to reflect the current port type (default), port speed, port operational state, or port transceiver media. Regardless of the default port view you choose, you can change the port view in the faceplate display by opening the View menu and selecting a different port view option. Refer to the corresponding subsection for more information:
  - ”Port Types” on page 5-2
  - ”Displaying Port Operational States” on page 5-3
  - ”Displaying Port Speeds” on page 5-3
  - ”Displaying Transceiver Media Status” on page 5-4

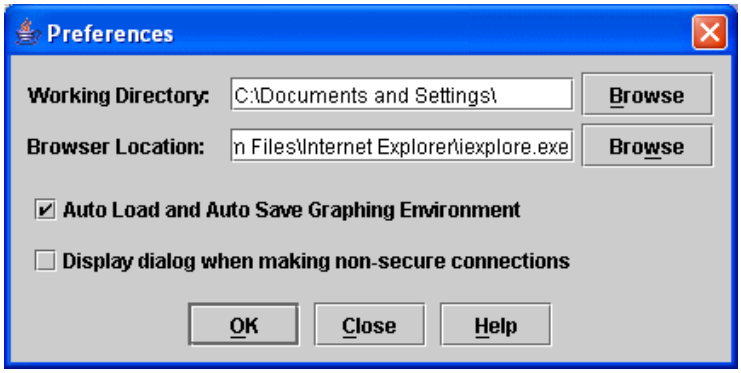


Figure 2-5. Preferences Dialog – SANsurfer Switch Manager

To set preferences for your SANsurfer Switch Manager sessions, do the following:

1. Open the File menu, and select **Preferences** to open the Preferences dialog.
2. Enter or browse for the path to the working directory and browser.
3. In the Application-Wide Options area, choose the preferences you want.
4. Click the **OK** button to save the changes.

2.9 Using Online Help

Online help is available for the SANsurfer Switch Manager application and its functions. The two ways to open the online help file are: open the Help menu and select **Help Topics**, or click the **Help** button in the tool bar. You can also display context-sensitive help for all SANsurfer Switch Manager dialogs by choosing the **Help** button in the dialog.

2.10 Viewing Software Version and Copyright Information

To view SANsurfer Switch Manager software version and copyright information, open the Help menu and select **About....**

2.11 SANsurfer Switch Manager User Interface

The SANsurfer Switch Manager application uses two basic displays to manage the fabric and individual switches: the topology display and the faceplate display. The topology display shows all switches that are able to communicate and all connections between switches. The faceplate display shows the front of a single switch and its ports. Both displays share some common elements as shown in Figure 2-6.

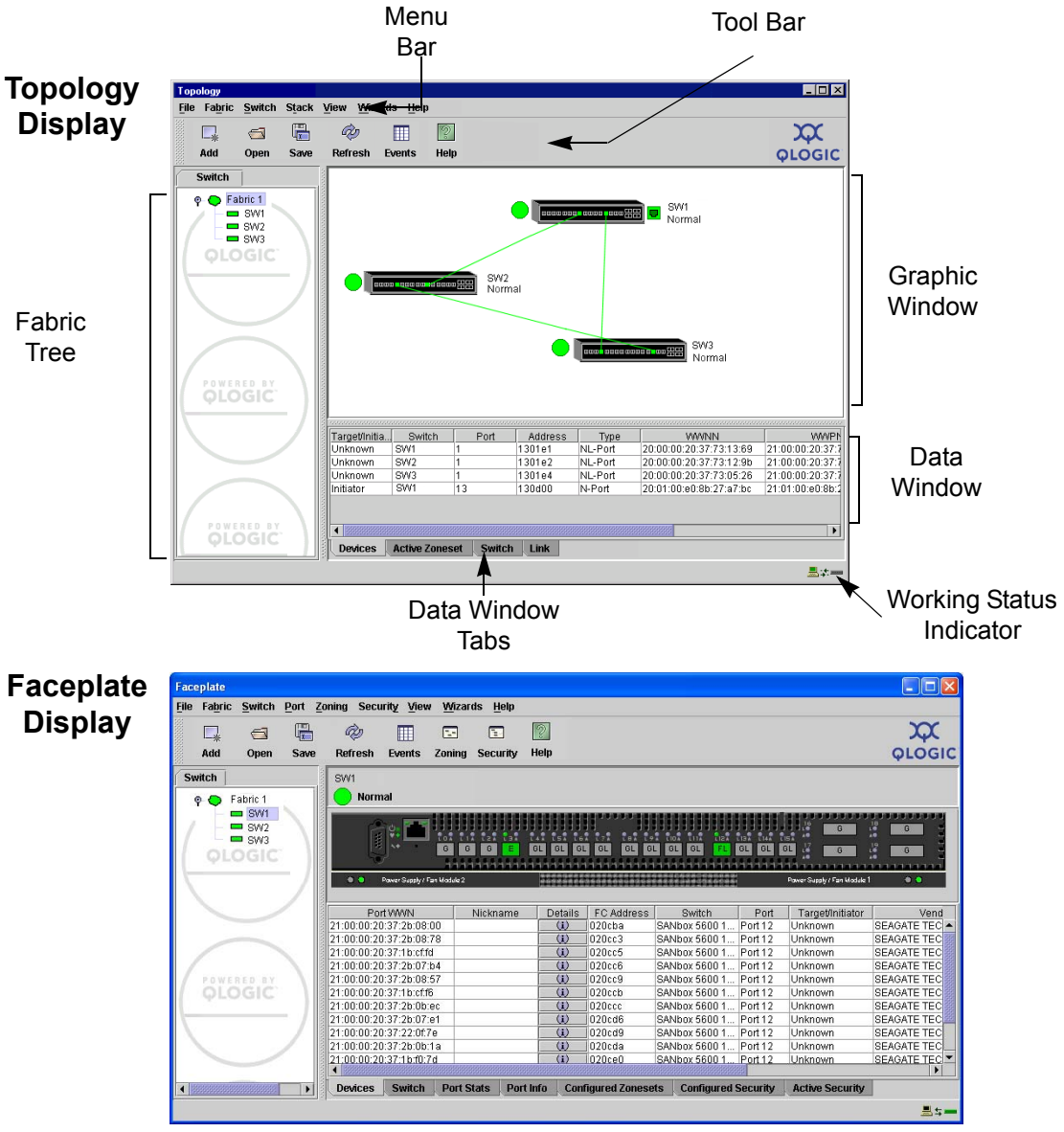


Figure 2-6. SANsurfer Switch Manager Display Elements

2.11.1
Menu Bars

The menus and the options offered in them vary depending on the display. For example, the Port menu and many of the Switch menu selections are available only in the faceplate display.

2.11.1.1
Topology Display Menu

The menu options available in the topology display are shown in Figure 2-7.

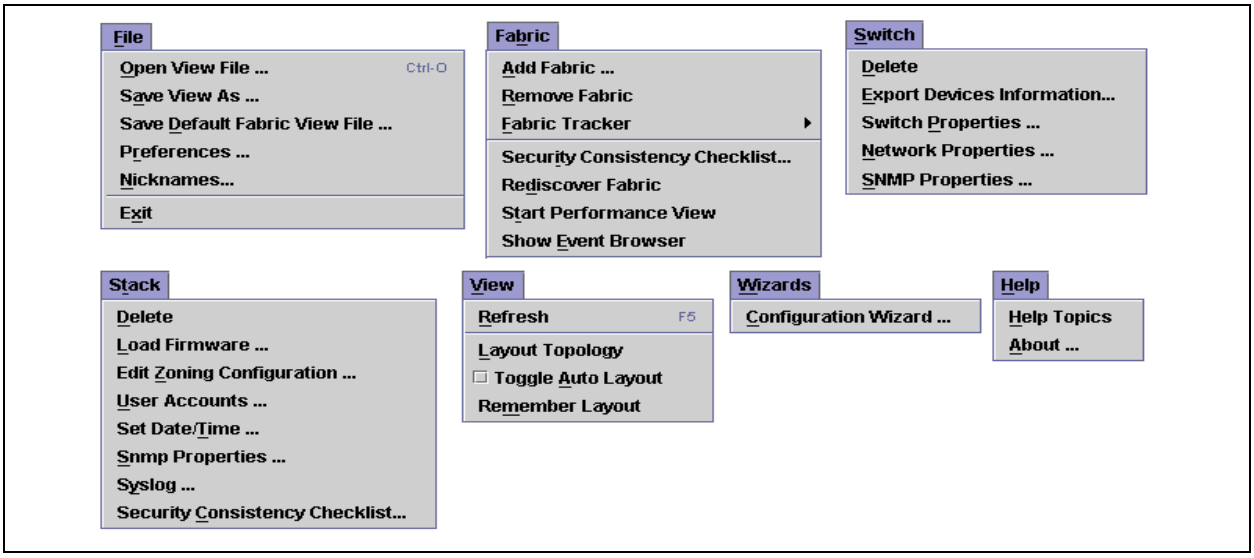


Figure 2-7. Topology Display Menu

2.11.1.2
Faceplate Display Menu

The menu options available in the faceplate display are shown in Figure 2-8.

Note: The Stack menu is displayed when the stack faceplate is displayed. The Switch menu is displayed when a a switch faceplate is displayed.

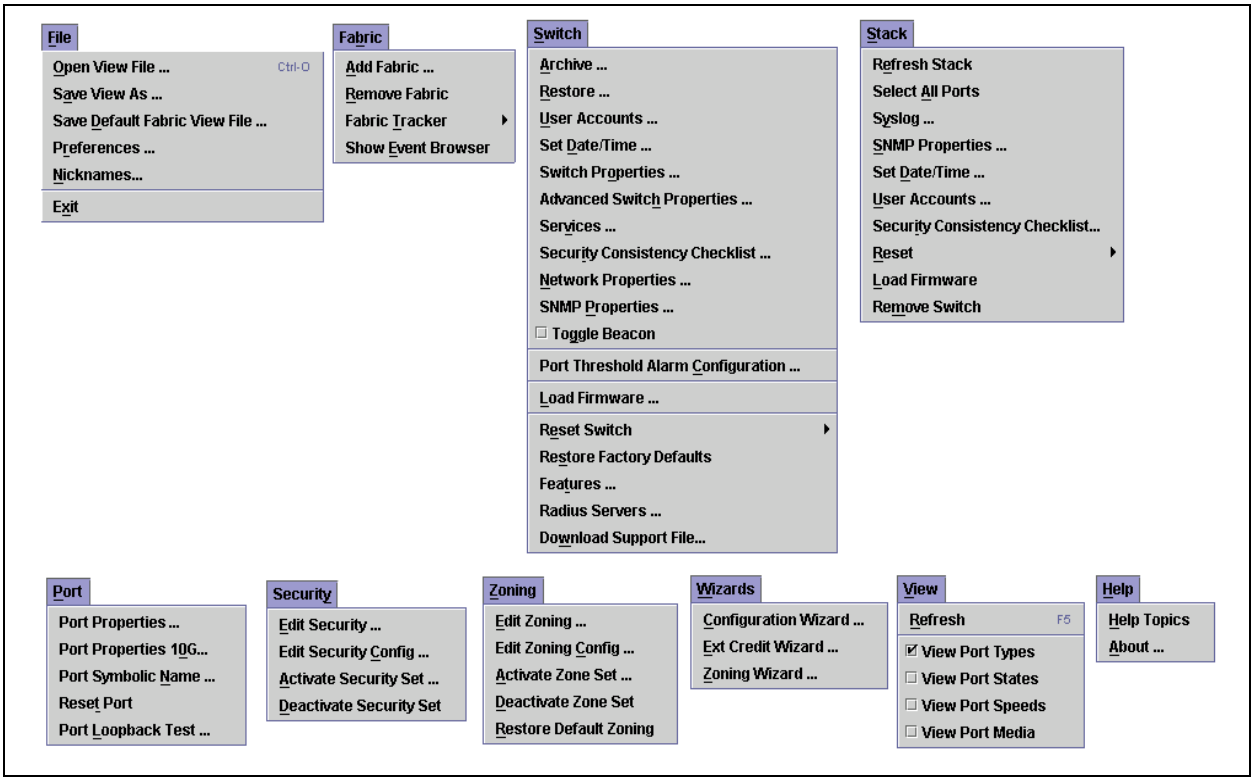


Figure 2-8. Faceplate Display Menu

The keyboard shortcut keys vary by display type: topology display and faceplate display. In addition to the menu bar, both the topology and faceplate displays have context sensitive menus that pop up when you right-click in the graphic window. Refer to ”Opening the Faceplate and Topology Display Popup Menus” on page 2-27 for more information about these popup menus.

2.11.1.3
Shortcut Keys

Shortcut key combinations, available in both the topology and faceplate displays, provide an alternative method of accessing menu options. The shortcut key combinations are not case-sensitive. For example, to exit the application, press **Alt+F**, then press **X**.

2.11.2
Tool Bar

The tool bar consists of a row of graphical buttons that you can use to access SANsurfer Switch Manager functions as shown in Table 2-2. The tool bar buttons are an alternative method to using the menu bar. The tool bar can be relocated in the display by clicking and dragging the handle at the left edge of the tool bar.

Table 2-2. Tool Bar Buttons

Tool Bar Button	Description
	Add Fabric button - adds a new fabric to the fabric view.
	Open View File button - opens an existing fabric view file.
	Save View As button - saves the current fabric view to a file.
	Refresh button - updates the topology or faceplate display with current information.
	Event Browser button - opens the events browser.
	Edit Zoning button - opens the Edit Zoning dialog (available only in faceplate display).
	Edit Security button - opens the Edit Security dialog (faceplate display only with SSL enabled)
	Help Topics button - opens the online help file.
	The QLogic logo opens a link to the QLogic web site.

2.11.3
Fabric Tree

The fabric tree lists the managed fabrics and their switches as shown in Figure 2-9. The window width can be adjusted by clicking and dragging the moveable window border. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded or collapsed. Click this handle or double-click the entry to expand or collapse a fabric tree entry. A fabric entry expands to show its member switches.

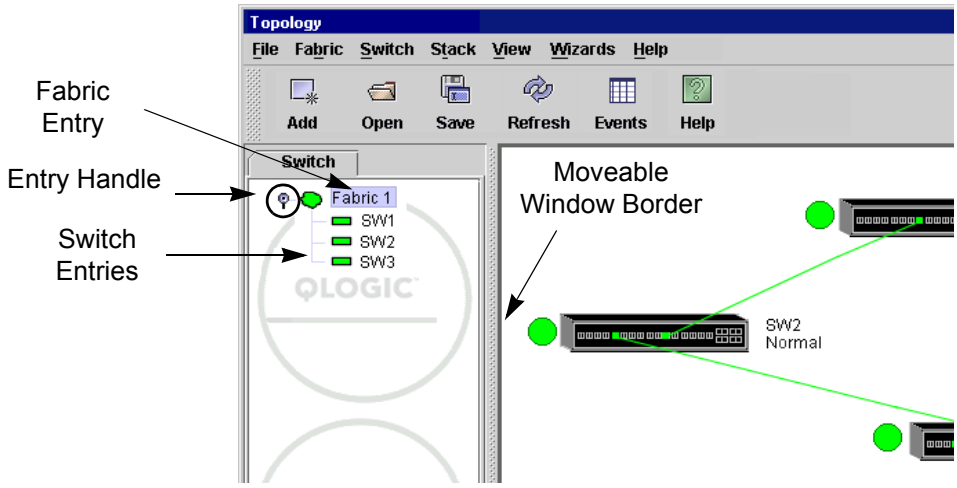


Figure 2-9. Fabric Tree

Each fabric tree entry has a small icon next to it that uses color to indicate operational status.

- A green icon indicates normal operation.
- A yellow icon indicates that a switch is operational, but may require attention to maintain maximum performance.
- A red icon indicates a potential failure or non-operational state as when the switch is offline.
- A blue icon indicates that a switch is unknown, unreachable, or unmanageable.

If the status of the fabric is not normal, the fabric icon in the fabric tree will indicate the reason for the abnormal status. The same message is provided when you rest the mouse over the fabric icon in the fabric tree.

The fabric tree provides access to the topology and faceplate displays for any fabric or switch.

- To open the topology display from the fabric tree, click a fabric entry.
- To open the faceplate display from the fabric tree, click a switch entry.

2.11.4
Graphic Window

The graphic window, as shown in Figure 2-6, presents graphic information about fabrics and switches such as the fabric topology and the switch faceplate. The window height can be adjusted by clicking and dragging the window border that it shares with the data window.

2.11.5
Data Window and Tabs

The data window presents a table of data and statistics associated with the selected tab. Use the scroll bar to browse through the data. The window length can be adjusted by clicking and dragging the border that it shares with the graphic window.

Adjust the column width by moving the pointer over the column heading border shared by two columns until a right/left arrow graphic is displayed. Click and drag the arrow to the desired width.

The data window tabs present options for the type of information to display in the data window. These options vary depending on the display.

2.11.6
Working Status Indicator

The working status indicator, located in the lower right corner of the SANsurfer Switch Manager window, shows when the management workstation is exchanging information with the fabric. As conditions change, the fabric forwards this information to the management workstation where it is reflected in the various displays.

2.12 Using the Topology Display

The topology display shown in Figure 2-10 receives information from the selected fabric and displays its topology. Switches and inter-switch links (ISLs) appear in the graphic window and use color to indicate status. Consider the following topology display features:

- Switch and Link Status
- Working with Switches and Links
- Topology Data Windows

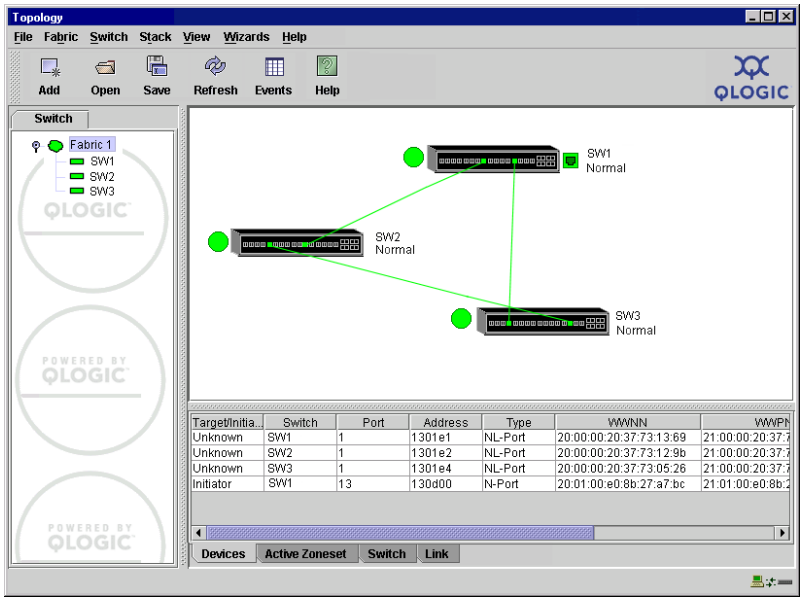


Figure 2-10. Topology Display

2.12.1 Switch and Link Status

Switch icon shape and color provide information about the switch and its operational state. Lines represent links between switches. The topology display uses green to indicate normal operation, yellow to indicate operational with errors, red to indicate a potential failure or non-operational state, and blue to indicate unknown, unreachable, or unmanageable. Refer to ”Fabric Status” on page 3-27 for more information about topology display icons.

2.12.2
Working with Switches and Links

Switch and link icons are selectable and moveable, and serve as access points for other displays and menus. You select switches and links to display information about them, modify their configuration, or delete them from the display. Context-sensitive popup menus are displayed when you right-click on a switch or link icon, or in the background of the topology display graphic window.

2.12.2.1
Selecting Switches and Links

Selected switch icons are highlighted in light blue. Selected ISLs are displayed as a heavier line. You can select switches and links in the following ways:

- To select a switch or a link, click the icon or link.
- To select multiple switches or links, hold down the Control key and select.
- To select all switches or links, right-click anywhere in the graphic window background. Select **Select All Switches** or **Select All Links** from the popup menu.

To cancel a selection, press and hold the Control key, and select the item again. To cancel all selections, click in the graphic window background.

2.12.2.2
Arranging Switches in the Display

You can arrange individual switch icons in the topology display or allow SANsurfer Switch Manager to arrange all switch icons for you:

- To move an individual switch icon, click and drag the icon to another location in the graphic window. Links stretch or contract to remain connected.
- To arrange all switch icons in the topology display automatically, open the View menu and select **Layout Topology**.

By default, the **Toggle Auto Layout** box in the View menu is checked which causes SANsurfer Switch Manager to arrange the icons when you select **Layout Topology**.

You can save a custom arrangement, or layout, and restore that layout during a SANsurfer Switch Manager session. Begin by arranging the icons, then open the View menu and select **Remember Layout**. To restore the saved layout, open the View menu, uncheck the **Toggle Auto Layout** box, and select **Layout Topology**.

2.12.2.3

Opening the Faceplate and Topology Display Popup Menus

The topology display shows all switches that are able to communicate and all connections between switches. The faceplate display shows the front of a single switch and its ports. Menu options vary with each type of popup menu.

- To open the fabric popup menu in the topology display, right-click the graphic window background.
- To open the switch popup menu in the topology display, right-click the switch icon in the graphic window.
- To open the link popup menu in the topology display, right-click the link.
- To open the switch popup menu in the faceplate display, right-click the faceplate in the graphic window.

2.12.3

Topology Data Windows

The topology display provides the following data windows corresponding to the data window tabs:

- Devices – displays information about devices (hosts and storage targets) connected to the switch. Refer to ”Devices Data Window” on page 3-33 for more information.
- Active Zoneset – displays the active zone set for the fabric including zones and their member ports. Refer to ”Active Zone Set Data Window” on page 3-34 for more information about this data window. Refer to ”Zoning a Fabric” on page 3-38 for information about zone sets and zones.
- Switch – displays current network and switch configuration data for the selected switches. Refer to ”Switch Data Window” on page 4-8 for more information.
- Link – displays information about the inter-switch links. Refer to ”Link Data Window” on page 3-35 to for more information.

2.13 Using the Faceplate Display

The faceplate display shown in Figure 2-11 displays the switch name and operational state, and port status. Consider the following functional elements of the faceplate display:

- Port Views and Status
- Working with Ports
- Faceplate Data Windows

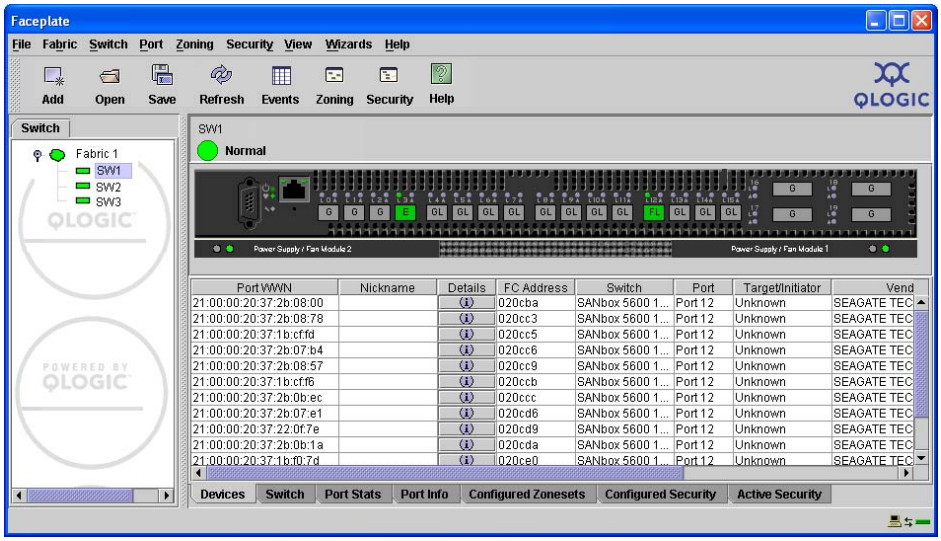

Faceplate
File Fabric Switch Port Zoning Security View Wizards Help
Add Open Save Refresh Events Zoning Security Help
QLOGIC
Switch
Fabric 1
SW1
SW2
SW3
SW1
Normal
Power Supply / Fan Module 2
Power Supply / Fan Module 1
Port WWN Nickname Details FC Address Switch Port Target/Initiator Vend
21:00:00:20:37:2b:08:00 020cba SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:08:78 020cc3 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:1b:cf:fd 020cc5 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:07:b4 020cc6 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:08:57 020cc9 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:1b:cf:f6 020ccb SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:0b:ec 020ccc SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:07:e1 020cd6 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:22:0f:7e 020cd9 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:0b:1a 020cda SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:1b:f0:7d 020ce0 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
Devices Switch Port Stats Port Info Configured Zonesets Configured Security Active Security

Figure 2-11. Faceplate Display

2.13.1 Port Views and Status

Port color and text provide information about the port and its operational state. Green indicates active; gray indicates inactive. The faceplate display provides the following views of port status corresponding to the View menu options in the faceplate display. Refer to ”Monitoring Port Status” on page 5-2 for more information about these displays.

- Port type
- Port state
- Port speed
- Port media

Context-sensitive popup menus are displayed when you right-click the faceplate image or a port icon in the faceplate display.

2.13.2
Working with Ports

Ports are selectable and serve as access points for other displays and menus. You select ports to display information about them in the data window or to modify them. Context-sensitive popup menus are displayed when you right-click the faceplate image or on a port icon in the faceplate display.

2.13.2.1
Selecting Ports

You can select ports in the following ways. Selected ports are outlined in white.

- To select a port, click the port in the faceplate display.
- To select a range of consecutive ports, select a port, then press and hold the shift key and select another port. The application selects both end ports and all ports in between in port number sequence.
- To select several non-consecutive ports, hold the Control key and select.
- To select all ports, right-click on the faceplate image. Select **Select All Ports** from the popup menu.

To cancel a selection, press and hold the Control key and select it again.

2.13.2.2
Opening the Faceplate Popup Menu

To open the popup menu, right-click on the faceplate image to present the following tasks.

- Refresh the switch
- Select all ports
- Manage switch properties
- Manage network properties
- Manage SNMP properties
- Extended credits wizard
- Manage port properties
- Change the port symbolic name
- Run the port loopback tests
- Services
- Security Consistency Checklist

If no ports are selected, the port-related tasks will be unavailable in the menu. Right-click a port to open the Port popup menu. Hold down the Shift or Control key to select more than one port. If multiple ports are selected, right-click one of the selected ports.

2.13.3
Faceplate Data Windows

The faceplate display provides the following data windows corresponding to the data window tabs:

- Devices – displays information about devices (hosts and storage targets) connected to the switch.
- Switch – displays current switch configuration data.
- Port Statistics – displays performance data for the selected ports.
- Port Information – displays information for the selected ports.
- Configured Zonesets – displays all zone sets, zones, and zone membership in the zoning database.
- Configured Security – displays all security definitions currently saved in the database.
- Active Security – displays the active security set.

Section 3

Managing Fabrics

This section describes the following tasks that manage fabrics:

- RADIUS Servers
- Securing a Fabric
- Tracking Fabric Firmware and Software Versions
- Managing the Fabric Database
- Displaying Fabric Information
- Working with Device Information and Nicknames
- Zoning a Fabric

3.1 RADIUS Servers

Remote Authentication Dial In User Service (RADIUS) provides a method to centralize the management of authentication passwords in larger networks. It has a client/server model, where the server is the password repository and third party authentication point and the clients are all of the managed devices. RADIUS can be configured for devices and/or user accounts. The RADIUS server dialogs are available only on a secure (SSL) fabric and on the entry switch (out of band switch). Refer to ”Connection Security” on page 3-7 and ”System Services Dialog” on page 4-25 for more information.

RADIUS is designed to authenticate users and devices using a challenge/response protocol. Basic implementations consist of a central RADIUS server containing a database of authorized users as well as authentication information. A RADIUS client wishing to verify the authenticity of a user issues a challenge to the user and collects the response to the challenge. This information is forwarded to the RADIUS server for authentication and the server responds with the results, either an accept or reject. The RADIUS client does not need to be configured with any user authentication information, this all resides on the RADIUS server and can be managed centrally and separately from the clients. In addition, no passwords are exchanged between the RADIUS server and its clients. Authentication of requests from a RADIUS client to the server and responses from the server to a client can also be authenticated. This requires sharing a secret between the server and client. The accounting RADIUS supports the auditing of the users and switch services such as Telnet, FTP, and switch management applications.

3.1.1
Adding a RADIUS Server

When you add a RADIUS server, you provide a method to centralize the management of authentication passwords over a network.

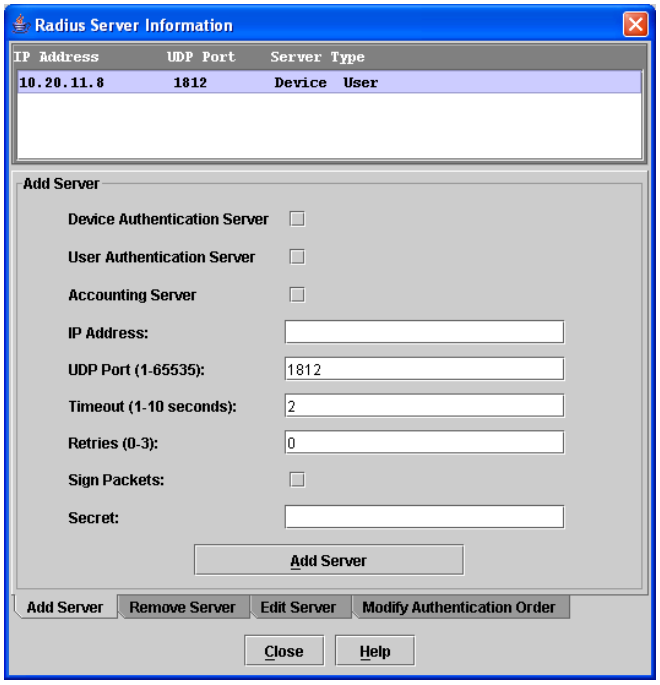


Figure 3-1. Add Radius Server

To add a RADIUS server, do the following:

1. Open the faceplate display, open the Switch menu, and select **Radius Servers...**.
2. In the Radius Server Information dialog, shown in Figure 3-1, click the **Add Server** tab.
3. Select the server type (Device, User, Account).
4. In the IP Address field, enter the remote IP address of the server.
5. In the UDP Port field, enter the remote UDP port number of the Authentication Radius Server. The Radius Accounting Server UDP port will always be the value of Device/User Authentication Server UDP Port + 1.
6. In the Timeout field, enter the timeout value in seconds (minimum of 1 second, maximum of 30 seconds). This is the number of seconds the RADIUS client will wait for a response from the RADIUS server before retrying, or giving up on a request.

7. In the Retries field, enter the the number of retries. This is the maximum number of times the RADIUS client will retry a request sent to the primary RADIUS server.
8. Select the Sign Packet check box to enable the switch to include a digital signature (Message-Authenticator) in all RADIUS access request packets sent to the RADIUS server. A valid Message-Authenticator attribute will be required in all RADIUS server responses.
9. In the Secret field, enter the server secret. A secret is required for all RADIUS servers. The secret is used when generating and checking the Message-Authenticator attribute.
10. Click the **Add Server** button to add the server, and click the **Close** button to exit the dialog.
11. Click the **Modify Authentication Order** tab, and verify that Device Authentication Order and User Authentication Order options are set to either **Radius** or **Radius Local** for Radius Authentication to be implemented.

3.1.2
Removing a RADIUS Server

When you remove a RADIUS server, you disable the management of authentication usernames and passwords over the network for that server.

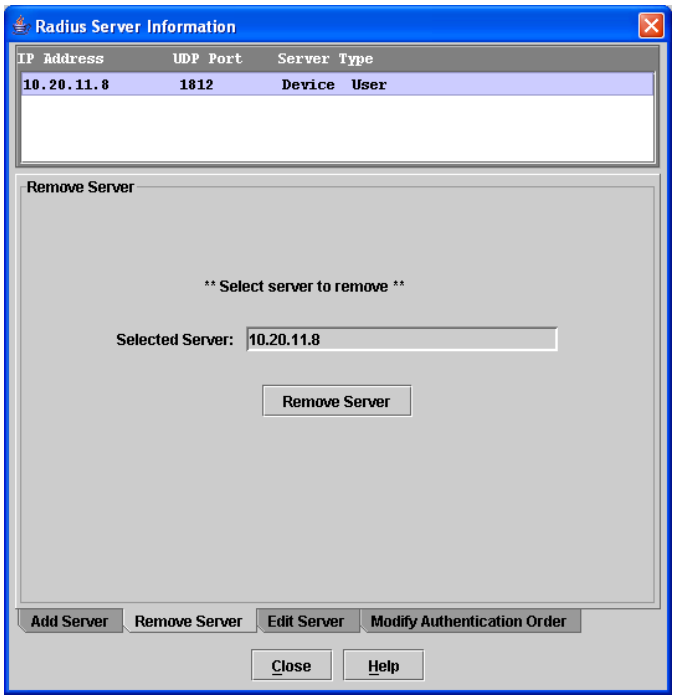


Figure 3-2. Remove Radius Server

To remove a RADIUS server, do the following:

1. Open the faceplate display, open the Switch menu, and select **Radius Servers...**.
2. In the Radius Server Information dialog, shown in Figure 3-2, click the **Remove Server** tab.
3. In server list at the top of the dialog, select the server to be removed.
4. Click the **Remove Server** button to remove the server, and click the **Close** button to exit the dialog.

3.1.3
Editing RADIUS Server Information

Editing information of a RADIUS server involves changing the configuration of a RADIUS server.

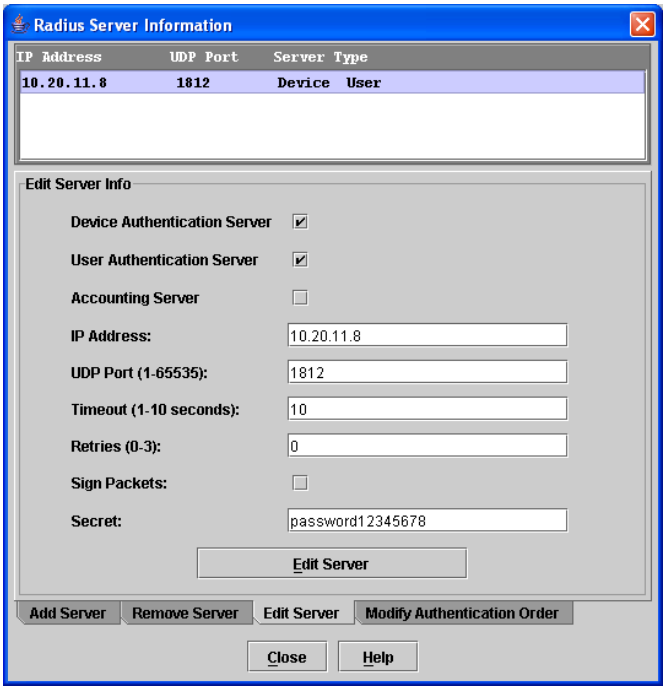


Figure 3-3. Edit Radius Server Information

To edit information of a RADIUS server, do the following:

1. Open the faceplate display, open the Switch menu, and select **Radius Servers...**.
2. In the Radius Server Information dialog, shown in Figure 3-3, click the **Edit Server** tab.
3. In server list at the top of the dialog, select the server to be edited.
4. Make changes to the IP Address, UDP Port, Timeout, Retries, and Secret fields.
5. Select or unselect the server type (Device, User, Account) and Sign Packet check boxes.
6. Click the **Edit Server** button to save the changes, and click the **Close** button to exit the dialog.

3.1.4
Modifying Authentication Order RADIUS Server Information

Editing information of a RADIUS server involves changing the configuration of a RADIUS server.

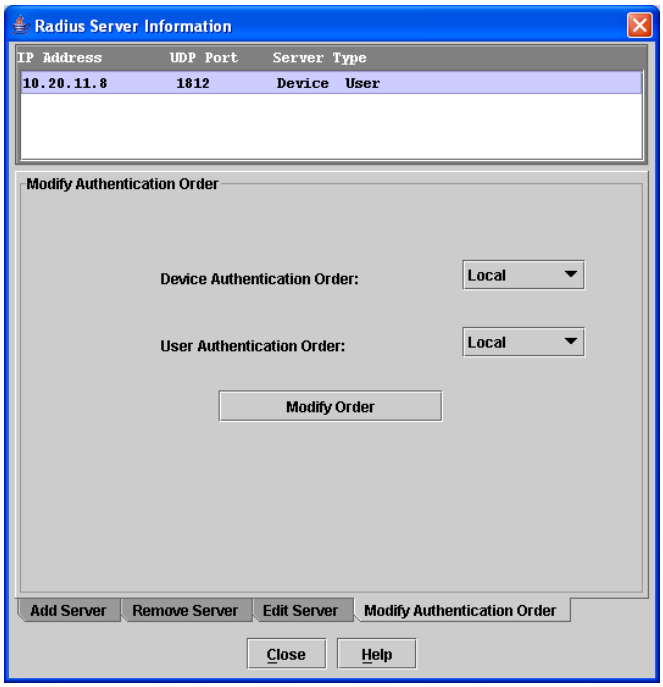


Figure 3-4. Modify Authentication Order - Radius Server Information

To modify the authentication order information of a RADIUS server, do the following:

1. Open the faceplate display, open the Switch menu, and select **Radius Servers...**.
2. In the Radius Server Information dialog, shown in Figure 3-4, click the **Modify Authentication Order** tab.
3. In server list at the top of the dialog, select the server to be modified.
4. Make changes to the Device Authentication Order or User Authentication Order pull-down menus. Select **Local**, **Radius**, or **Radius Local**.
5. Click the **Modify Order** button to save the changes, and click the **Close** button to exit the dialog.

3.2 Securing a Fabric

Fabric security consists of the following:

- Connection Security
- User Account Security
- Security Consistency Checklist
- Device Security
- Fabric Services

3.2.1 Connection Security

Connection security provides an encrypted data path for switch management methods. The switch supports the Secure Shell (SSH) protocol for the command line interface and the Secure Socket Layer (SSL) protocol for management applications such as SANsurfer Switch Manager and Common Information Module (CIM).

The SSL handshake process between the workstation and the switch involves the exchanging of certificates. These certificates contain the public and private keys that define the encryption. The switch certificate is valid for one year beginning with its creation date and time. The workstation validates the switch certificate by comparing the workstation date and time to the switch certificate creation date and time. For this reason, it is important to snychronize the workstation and switch with the same date, time, and time zone. If a certificate has not been created by the user, the switch will automatically create one.

Consider your requirements for connection security: for the command line interface (SSH), management applications such as SANsurfer Switch Manager (SSL), or both. If SSL connection security is required, also consider using the Network Time Protocol (NTP) to synchronize workstations and switches.

3.2.2
User Account Security

User account security is the process by which your user account and password are authenticated with the list of valid user accounts and passwords. The switch validates your account and password when you attempt to add a fabric using SANsurfer Switch Manager or log in to a switch through Telnet. Your system administrator defines accounts, passwords, and authority levels that are stored on the switch. Refer to ”Managing User Accounts” on page 4-1 for more information.

The Admin account possesses Admin authority which grants full access to all tasks of the SANsurfer Switch Manager menu system. The switch validates your user account and SANsurfer Switch Manager grants access to its menus according to your authority level. If you do not have Admin authority, you are limited to monitoring tasks.

Note: If a user is logged into a switch using SANsurfer Switch Manager or CLI, and an administrator changes user access rights and passwords, existing logins will not be affected by the new settings. Login access and privileges are only checked for a new login request.

3.2.3
Security Consistency Checklist

The Security Consistency Checklist dialog enables you to compare security-related features on switches to check for inconsistencies. Any changes must be made through the appropriate dialog, such as Network Properties dialog, Switch Properties dialog, or SNMP Properties dialog. To open the Security Consistency Checklist dialog, open the Switch menu and select **Security Consistency Checklist**.

3.2.4
Device Security

Device security provides for the authorization and authentication of devices that you attach to a switch. You can configure a switch with a group of devices against which the switch authorizes new attachments by devices, other switches, or devices issuing management server commands. Device security is configured through the use of security sets and groups. A group is a list of device worldwide names that are authorized to attach to a switch. There are three types of groups: one for other switches (ISL), another for devices (port), and a third for devices issuing management server commands (MS). A security set is a set of up to three groups with no more than one of each group type. The security configuration is made up of all security sets on the switch.

In addition to authorization, the switch can be configured to require authentication to validate the identity of the connecting switch, device, or host. Authentication can be performed locally using the switch security database, or remotely using a Remote Dial-In User Service (RADIUS) server. With a RADIUS server, the security database for the entire fabric resides on the server. In this way, the security database can be managed centrally, rather than on each switch. You can configure up to five RADIUS servers to provide failover.

You can configure the RADIUS server to authenticate just the switch or both the switch and the initiator device if the device supports authentication. When using a RADIUS server, every switch in the fabric must have a network connection. A RADIUS server can also be configured to authenticate user accounts.

Consider the devices, switches, and management agents and evaluate the need for authorization and authentication. Also consider whether the security database is to distributed on the switches or centralized on a RADIUS server and how many servers to configure.

Managing device security involves the following tasks:

- Creating security sets, groups, and members
- Editing a security configuration on a switch
- Viewing properties of a security set, group, or member
- Archiving a security configuration on a switch to a file
- Activating and deactivating a security set

The security database is made up of all security sets on the switch. The security database has the following limits:

- Maximum number of security sets is 4.
- Maximum number of groups is 1000.
- Maximum number of members in a group is 1000.
- Maximum total number of group members is 1000.

3.2.4.1
Edit Security Dialog

The Edit Security dialog, shown in Figure 3-5 opens after clicking the Security button on the toolbar or selecting Edit Security from the Security menu. The Security dialogs are available only on a secure (SSL) fabric and on the entry switch (out of band switch). The primary use of the Edit Security dialog is to edit the security configuration on the switch. You can also open and edit a security configuration saved to a file. Editing security files consists of renaming and removing security sets, groups, and members.

Use the Edit menu options or popup menu options to access Edit Security dialog options. Select a security item in the graphic window and select an option in the Edit menu, or right-click on a security item in the graphic window, and select an option from the popup menus.

The orphan security set contains the security groups and members that don't belong to a user-defined security set. Excluding the orphan security set, you can only have 1 group type in a security set. The three types of security groups are:

- ISL - default (E_Port authentication)
- MS (Management Server CT authentication)
- Port (F_Port authentication)

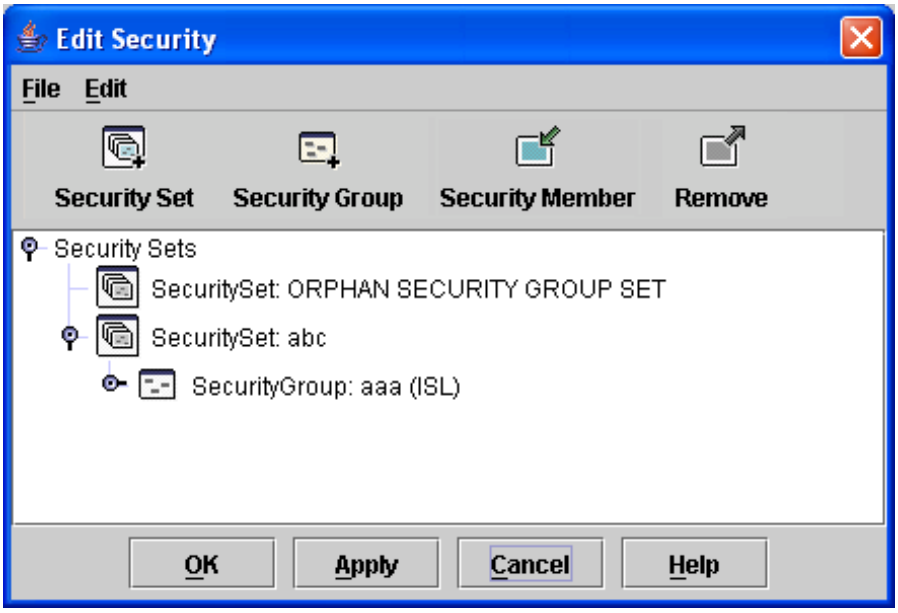


Figure 3-5. Edit Security Dialog

Use the File menu to:

- Edit the security configuration on the switch.
- Open or edit security files.
- Save or rename security files

Use the Edit menu to:

- Create security sets, security groups, and security group members
- Rename or remove a security group from a security set or a member from a security group
- Remove a group from all security sets
- Remove all security sets, groups, or members
- View properties for the selected security set, group, or group memberCreating a Security SetCreating a Security Set

3.2.4.2

Creating a Security Set

There is a maximum of 4 security sets. To add a security set, do the following:

1. On the faceplate display, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security dialog.
2. Choose one of the following methods to open the Create a Security Set dialog:
   - Click the **Security Set** button in the toolbar.
   - Right-click in the graphic window, and select **New Security Set** from the popup menu.
3. Enter a security set name. The naming conventions for security sets are:
   - Must start with a letter
   - All alphanumeric chars [aA- zZ] [0-9]
   - The symbols $ _ - and ^ are the only symbols allowed
4. Click the **OK** button to save the change.

3.2.4.3
Create Security Group Dialog

Use the Create Security Group dialog, shown in Figure 3-6, to add a security group to a security set. The Create Security Group dialog is displayed after clicking the Security Group button on the toolbar, or after you right-click on a security set in the graphic window and select Create a Security Group from the popup menu.

Figure 3-6. Create Security Group Dialog

The naming conventions for all security groups are listed below.

- Must start with a letter
- All alphanumeric chars [aA- zZ] [0-9]
- The symbols $ _ - and ^ are the only symbols allowed

3.2.4.4

Creating a Security Group

An empty (no members) security group in the active security set will prevent all connections for that security group type. For example, an empty ISL security group will cause the switch to refuse all logins from other switches. To add a security group to a security set, do the following:

1. On the faceplate display, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security dialog.
2. Choose one of the following methods to open the Create a Security Group dialog:
   - In the graphic window, click a security set and click the **Security Group** button in the toolbar.
   - Right-click on a security set and select **Create a Security Group** from the popup menu.
3. Enter a security group name and select a security group type (ISL, Port, or MS). Remember, only one security group type (1 ISL, 1 Port, 1 MS) in each security set is allowed. The naming conventions for security groups are:
   - Must start with a letter
   - All alphanumeric chars [aA- zZ] [0-9]
   - The symbols $ _ - and ^ are the only symbols allowed
4. Click the **OK** button to save the change.

3.2.4.5
Create Security Group Member Dialog

Use the Create Security Group Member dialog, shown in Figure 3-7, to add a member to a security group. Choose options from the Group Member (or manually type in a hex value) and Authentication pull-down menus, and enter values in the Secret and Binding (ISL groups only) fields.

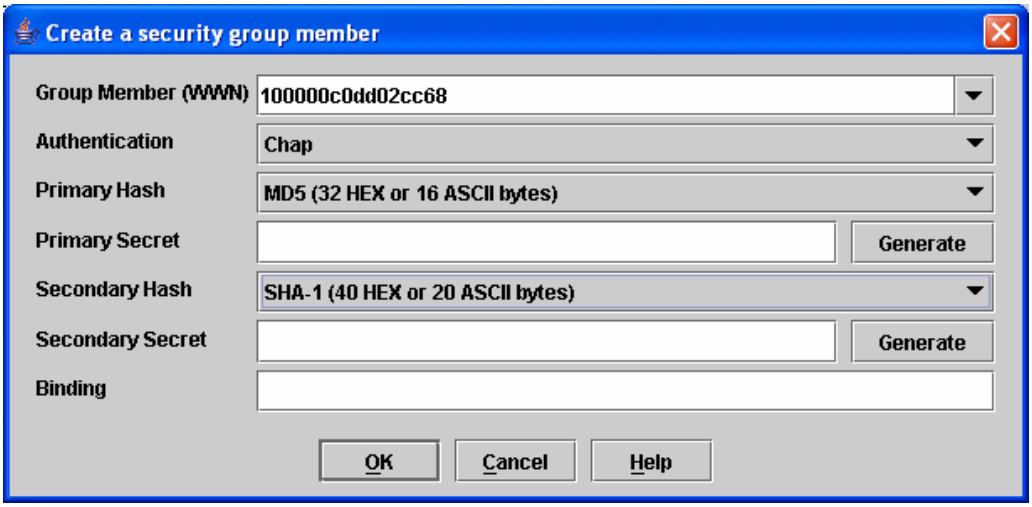


Figure 3-7. Create a Security Group Member Dialog

The conventions for ISL security group members are listed below:

- You can enter member world-wide name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The authentication choices are None and Chap.
- The Secret field is disabled if authentication is set to None. If authentication is Chap, the Secret field is enabled.
- The **Generate** button is only enabled when authentication is set to Chap.
- Valid binding entries are between 0 to 239.

The conventions for Port security group members are listed below:

- You can enter member world-wide name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The authentication choices are None and Chap.
- The Secret field is disabled if authentication is set to None. If authentication is Chap, the Secret field is enabled.
- The **Generate** button is only enabled when authentication is set to Chap.

The conventions for MS security group members are listed below:

- You can enter member world-wide name (WWN), which must be 16 hex characters, or 23 characters with valid WWN format xx:xx:xx:xx:xx:xx:xx:xx.
- The CT (common transport) authentication choices are None, MD5, and SHA-1.
- The Secret field is disabled if authentication is set to None, otherwise the Secret field enabled.
- The **Generate** button is only enabled when authentication is Chap.
- Secret is 16 byte length for MD5 authentication, and 20 bytes if authentication is SHA-1.

3.2.4.6

Creating a Security Group Member

To add a member to a security group, do the following:

1. On the faceplate display, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security dialog.
2. Choose one of the following methods to open the Create a Security Group Member dialog:
   - In the graphic window, click a security group and click the **Security Member** button in the toolbar.
   - Right-click on a security group and select **Create Members** from the popup menu.
3. Open the Group Member pull-down menu and select a Node World-Wide Name. The switch must be a member of any group in which authentication is used. You can also type in a hex value.
4. Open the Authentication pull-down menu, and select a type of protocol to be used for the authentication process for that member.
   - ISL authentication options are None (0 bytes), Chap (16 bytes)
   - MS (CT - Common Transport) authentication options are None (0 bytes), MD5 (16 bytes), SHA (20 bytes)
   - Port authentication options are None (0 bytes), Chap (16 bytes)
5. In the Secret area, enter an authentication "password" to be assigned that member. Or, you can click the **Generate Secret** button to randomly generate a secret.
6. In the Binding field (ISL groups only), enter the domain ID (1-239) for the switch for the ISL group member. The WWN of the switch must be at the entered domain ID when attempting to enter the fabric, otherwise it will become isolated.
7. Click the **OK** button to save the changes.

3.2.4.7
Editing the Security Configuration on a Switch

To edit a security configuration on the switch, do the following:

1. On the faceplate display, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security dialog. By default, the security configuration on the switch is displayed in the Edit Security dialog. To edit a security configuration saved to a file, open the File menu and select **Open File**, or press **Ctrl+o** (letter o) to open the Open dialog. Browse for and select the security file, and click the **Open** button to display the security file in the Edit Security dialog.
2. Select the security item to edit in the graphic window, and choose one of the following:
   - **Rename a Security Set, or Group**. Open the Edit menu and select a Rename option. In the Rename dialog, enter a new name and click the **OK** button to save the changes.
   - **Edit Security Group Member**. Open the Edit menu and select a Edit Security Group Member option. In the Edit Security Group Member dialog, enter a new Group Member (WWN), choose an option in the Authentication pull-down menu, and click the **OK** button to save the changes.
   - **Remove a Security Set, Group, or Member**. Select the item to remove, open the Edit menu and select a Remove option. In the Remove dialog, click the **OK** button to remove that item from the security file and save the changes.
   - **Clear Security**. Select the Security Sets directory name, open the Edit menu and select **Clear Security**. In the Remove dialog, click the **OK** button to remove all security sets and save the changes. You can also right-click on the Security Sets (top level) directory name, and select **Clear Security** from the popup menu, and click the **OK** button to remove all security sets.
3. Click the **Apply** button to save the changes and keep the Edit Security dialog open. To save changes and close the Edit Security dialog in one step, click the **OK** button.
4. Click the **OK** button to close the Edit Security dialog.

3.2.4.8
Viewing Properties of a Security Set, Group, or Member

To view the properties of a security set, group, or member, do the following:

1. On the faceplate display and click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security dialog.
2. Choose one of the following:
   - Select a security set, group, or member, open the Edit menu and select **Properties**.
   - In the graphic window, right-click on the security item, and select **Properties** from the popup menu.
3. View the security information for the selected item in the Properties dialog.

3.2.4.9
Using the Security Config Dialog

Use the Security Config dialog, shown in Figure 3-8, to save the active security configuration on the switch to non-volatile or to temporary memory, and to require the domain ID of a switch be validated before attaching to the fabric.

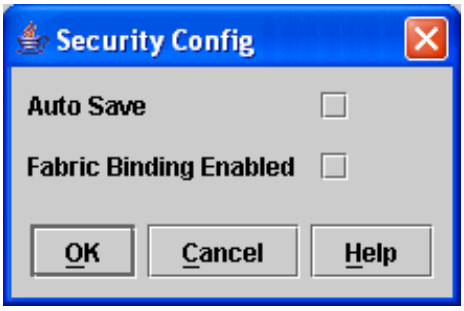


Figure 3-8. Security Config Dialog

To configure security on the switch, do the following:

1. On the faceplate display, open the Security menu and select **Edit Security Config** to open the Security Config dialog.
2. Check the **Auto Save** check box to enable (default) or disable Auto Save mode. If enabled, the security configuration is saved to non-volatile memory on the switch. If disabled, the security file is saved only to temporary memory. The Auto Save feature is used when Fabric Binding is enabled. When Auto Save is disabled, any updates from remote switches will not be saved locally. If the local switch is reset, it may isolate.

3. Check the **Fabric Binding Enabled** check box to require the expected domain ID of a switch is verified before being allowed to attach to the fabric.

Note: The fabric binding feature **must** be enabled on all switches in the fabric. When enabling this feature, it is best to set the switch state to offline, enable the fabric binding feature on all switches, and then set the switch state to online.

4. Click the **Apply** button to save the settings.
5. Click the **OK** button to close the Security Config dialog.

3.2.4.10

Archiving a Security Configuration to a File

To archive (save) a security configuration to a file, do the following:

1. On the faceplate display, click the **Security** button on the toolbar, or open the Security menu and select **Edit Security** to open the Edit Security dialog.
2. Configure the security settings as desired.
3. Open the File menu and select **Save As**.
4. In the Save dialog, enter a name and location for the security file (.xml extension).
5. Click the **Save** button to save the security file.

3.2.4.11

Activating a Security Set

Only one security set can be active at one time. To activate a security set, do the following:

1. On the faceplate display, open the Security menu and select **Activate Security Set** to open the Activate Security Set dialog.
2. In the Activate Security Set dialog, select a security set from the pull-down menu.
3. Click the **Activate** button to activate the security set.

3.2.4.12

Deactivating a Security Set

Only one security set can be active at one time. To deactivate an active security set, do the following:

1. In the faceplate display, open the Security menu and select **Deactivate Security Set**.
2. In the Deactivate dialog, click the **Yes** button to confirm that you want to deactivate the active security set.

3.2.4.13
Configured Security Data Window

The Configured Security data window displays a graphical representation of all security sets, groups, and members in the database. To open the Configured Security data window, click the **Configured Security** tab below the data window in the faceplate display.

3.2.4.14
Active Security Data Window

The Active Security data window displays a graphical representation of the active security set, its groups, and members in the database. To open the Active Security data window, click the **Active Security** tab below the data window in the faceplate display.

3.2.5
Fabric Services

Fabric services security includes SNMP and In-band management. Simple Network Management Protocol (SNMP) is the protocol governing network management and monitoring of network devices. SNMP security consists of a read community string and a write community string, that are basically the passwords that control read and write access to the switch. The read community string ("public") and write community string ("private") are set at the factory to these well-known defaults and should be changed if SNMP is enabled using the System Servieces or SNMP Properties dialogs. If SNMP is enabled (default) and the read and write community strings have not been changed from their defaults, you risk unwanted access to the switch. Refer to ”Enabling SNMP Configuration” on page 3-20 for more information. SNMP is enabled by default.

In-band management is the ability to manage switches across inter-switch links using SANsurfer Switch Manager, SNMP, management server, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection. Refer to ”Enabling In-band Management” on page 3-20 for more information.

3.2.5.1
Enabling SNMP Configuration

To enable SNMP configuration, choose one of the following:

1. On the faceplate display, open the Switch menu.
   - Select **SNMP Properties** to open the SNMP Properties dialog. In the SNMP Configuration area, place a check mark in the **SNMP Enabled** check box.
   - Select **Services** to open the System Services dialog. Check the **SNMP** option.
2. Click the **OK** button to save the change to the database.

3.2.5.2
Enabling In-band Management

To enable In-band Management, do the following:

1. On the faceplate display, open the Switch menu and select **Switch Properties** to open the Switch Properties dialog.
2. Click the **In-band Management Enable** button.
3. Click the **OK** button to save the change to the database.

3.3
Tracking Fabric Firmware and Software Versions

The Fabric Tracker option enables you to generate a snapshot or baseline of current system version information, which can be viewed, analyzed and compared to other snapshot files, and exported to a file. Information includes date and time, SANsurfer Switch Manager version, switch active firmware version, device hardware, drivers, and firmware version from FDMI.

The Snapshot Analyzer option enables you to:

- Compare two snapshots
- Detect mismatches of firmware and driver versions
- Detect devices that have been moved, added to or removed from the fabric.

3.3.1
Saving a Version Snapshot

To save the current snapshot to an XML file, open the Fabric menu, select **Fabric Tracker**, and select **Save Snapshot**. To view and analyze system version information, open the Fabric menu, select **Fabric Tracker**, and select **Analyze Snapshots**. The Fabric Version Snapshot Analysis dialog, shown in Figure 3-9, opens with the Summary, Differences and Reports tab pages. Click the **Browse** buttons to open and view the snapshot files in the corresponding tab pages. Click the **Close** button to exit the Fabric Version Snapshot Analysis dialog. The color key below the scrollable area defines the meanings of the colors used.

The Summary tab page shows a brief description of the changes that have occurred between the older snapshot and the newer one. Use the Summary tab page quickly view what has changed.

3.3.2 Viewing and Comparing Version Snapshots

The Differences tab page shows a side-by-side comparison of two snapshots. The timestamp of each snapshot is displayed above the scroll area showing that snapshot. The background color of the older snapshot is darker than the background of the newer snapshot. The arrow icon between the snapshot selectors always points from the older snapshot to the newer one. If the two snapshots have the same timestamp, the arrow will not be displayed. The scroll bars are synchronized to view the same portion of each snapshot file simultaneously. Click and drag the separator bar between the two panes to resize each pane. At the top of the separator bar between the two panes, click the left/right arrows to close the corresponding pane. The left/right arrows move to one side.

3.3.3 Exporting Version Snapshots to a File

The Reports tab page enables you to select one of several reports to save to a text file. The are two types of reports. The Summary report type shows the same format displayed on the Summary tab page without the color highlighting. The Detail report type shows a detailed breakdown of the differences. Use the **Export** button to save the selected report to a text file.

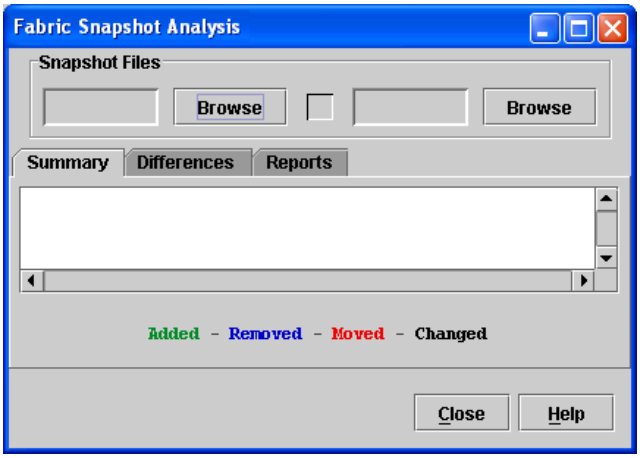


Figure 3-9. Fabric Version Snapshot Analysis Dialog

3.4 Managing the Fabric Database

A fabric database contains the set of fabrics that you have added during a SANsurfer Switch Manager session. Initially, if you do not open an existing fabric or fabric view file, the SANsurfer Switch Manager application opens with an empty fabric database.

3.4.1 Adding a Fabric

To add a fabric to the database, do the following:

1. Open the Fabric menu and select **Add Fabric** to open the Add a New Fabric dialog shown in Figure 3-10.

Figure 3-10. Add a New Fabric Dialog

2. Enter a fabric name (optional) and the IP address of the switch through which to manage the fabric.
3. Enter an account name and password. The factory account name and password are "admin" and "password". The password is for the switch and is stored in the switch firmware. Refer to ”Managing User Accounts” on page 4-1 or the ”User Command” on page A-123 for information about creating user accounts.

Note: A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SANsurfer Switch Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

4. Click the **Add Fabric** button.

Note: If the entry switch has SSL (Secure Socket Layer) enabled, the switch will generate and display a Verify Certificate dialog that you must accept before gaining access to the fabric. Refer to ”Connection Security” on page 3-7 and ”System Services Dialog” on page 4-25 for more information on certificates and SSL.

3.4.2 Removing a Fabric

To delete a fabric file from the database, do the following:

1. Select a fabric in the fabric tree.
2. Open the Fabric menu and select **Remove Fabric**.

3.4.3 Opening a Fabric View File

A fabric view file is one or more fabrics saved to a file. To open an existing view file, do the following:

1. Open the File menu and select **Open View File**, or click the **Open** button. If the fabric you are currently viewing has changed, you will be prompted to save the changes to the fabric view file with the Save View dialog before opening a different view file.
2. In the Open View dialog, enter the name of the file to open, and enter a file password, if a password was entered when this fabric view file was saved.
3. Click the **OK** button.

3.4.4
Saving a Fabric View File

To save a fabric view file, do the following:

1. Open the File menu, and select **Save View As**.
2. In the Save View dialog, enter a new file name.
3. Enter a file password, if necessary.
4. Click the **OK** button.

3.4.5
Rediscovering a Fabric

After making changes to or deleting switches from a fabric view, it may be helpful to again view the actual fabric configuration. The rediscover fabric option clears out the current fabric information being displayed, and rediscovers all switch information. To rediscover a fabric, open the Fabric menu, and select **Rediscover Fabric**. The rediscover function is more comprehensive than the refresh function.

3.4.6
Deleting Switches and Links

The SANsurfer Switch Manager application does not automatically delete switches or links that have failed or have been physically removed from the fabric. In these cases, you can delete switches and links to bring the display up to date. If you delete a switch or a link that is still active, the SANsurfer Switch Manager application will restore it automatically. You can also refresh the display. To delete a switch from the topology display, do the following:

1. Select one or more switches in the topology display.
2. Open the Switch menu and select **Delete**.

To delete a link, do the following:

1. Select one or more links in the topology display.
2. Open the Switch menu and select **Delete**.

3.4.7
Adding a New Switch to a Fabric

If there are no special conditions to be configured for the new switch, simply plug in the switch and the switch becomes functional with the default fabric configuration. The default fabric configuration settings are:

- Fabric zoning is sent to the switch from the fabric.
- All 1-Gbps/2-Gbps/4-Gbps ports will be GL_Ports; all 10-Gbps ports will be G_Ports.
- The default IP address 10.0.0.1 is assigned to the switch without a gateway or boot protocol configured (RARP, BOOTP, and DHCP).

If you are adding a new switch to a fabric and do not want to accept the default fabric configuration, do the following:

1. If the switch is not new from the factory, reset the switch to the factory configuration before adding the switch to the fabric by selecting **Restore Factory Defaults** in the Switch menu from the faceplate display.
2. If you want to manage the switch through the Ethernet port, you must first configure the IP address using the Network Properties dialog or the Configuration Wizard.
3. Configure any special switch settings. Consider configuring the Default Visibility setting to None in the Zoning Config dialog to prevent devices from finding other devices on all switches in the fabric until the new switch is configured. To open the Zoning Config dialog, open the Zoning menu, and select **Edit Zoning Config**.
4. Plug in the inter-switch links (ISL), but do not connect the devices.
5. Configure the port types for the new switch using the Port Properties dialog. The 1-Gbps/2-Gbps/4-Gbps ports can be G_Port, GL_Port, F_Port, FL_Port, or Donor. The 10-Gbps ports can be a G_Port or F_Port.
6. Connect the devices to the switch.
7. Make any necessary zoning changes using the Edit Zoning dialog. To open the Edit Zoning dialog, open the Zoning menu, and select **Edit Zoning**. If you changed the Default Visibility setting in the Zoning Config dialog from All to None, change that setting back to All. To open the Zoning Config dialog, open the Zoning menu, and select **Edit Zoning Config**.

3.4.8
Replacing a Failed Switch

The archive/restore works for all switches. However, the Restore menu item is not available for the in-band switches. You can only restore a switch out-of-band (the fabric management switch). There are certain parameters that are not archived, and these are not restored by SANsurfer Switch Manager. Refer to ”Archiving a Switch” on page 4-36 and ”Restoring a Switch” on page 4-37 for information about archive and restore. Use the following procedure to replace a failed switch for which an archive is available.

1. At the failed switch:
   a. Turn off the power and disconnect the AC cords.
   b. Note port locations and remove the interconnection cables and SFPs.
   c. Remove the failed switch.
2. At the replacement switch:
   a. Mount the switch in the location where the failed switch was removed.
   b. Install the SFPs using the same ports as were used on the failed switch.

      CAUTION! Do not reconnect inter-switch links, target devices, and initiator devices at this time. Doing so could invalidate the fabric zoning configuration.

   c. Attach the AC cords and power up the switch.
3. Select the failed switch in the topology display. Open the Switch menu and select **Delete**.
4. Restore the configuration from the failed switch to the replacement switch:
   a. Open a new fabric through the replacement switch.
   b. Open the faceplate display for the replacement switch. Open the Switch menu and select **Restore**.
   c. In the Restore dialog, enter the archive file from the failed switch or browse for the file.
   d. Click the **Restore** button.
5. Reset the replacement switch to activate the configuration formerly possessed by the failed switch including the domain ID and the zoning database. Open the Switch menu and select **Reset Switch**.
6. Reconnect the inter-switch links, target devices, and initiator devices to the replacement switch using the same ports as were used on the failed switch.

3.5 Displaying Fabric Information

The topology display is your primary tool for monitoring a fabric. The graphic window of the topology display provides status information for switches, inter-switch links, and the Ethernet connection to the management workstation.

The data window tabs show device, switch, and active zone set information. The Active Zoneset tab shows the zone definitions for the active zone set. Refer to ”Devices Data Window” on page 3-33 and ”Switch Data Window” on page 4-8 for information about the Devices and Switch data windows.

3.5.1 Fabric Status

The fabric updates the topology and faceplate displays by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the display status, or you can refresh the display at any time. To refresh the topology display, do one of the following:

- Click the **Refresh** button.
- Open the View menu and select **Refresh**.
- Press the F5 key.
- Right-click anywhere in the background of the topology display and select **Refresh Fabric** from the popup menu.

The topology display uses switch and status icons to provide status information about switches, inter-switch links, and the Ethernet connection. The switch status icons, displayed on the left side of a switch, vary in shape and color. Switches controlled by an Ethernet Internet Protocol have a colored Ethernet icon displayed on the right side of the switch. A green Ethernet icon indicates normal operation, yellow indicates a condition that may require attention to maintain maximum performance, and red indicates a potential failure. Table 3-1 shows the different switch icons and their meanings.

Table 3-1. Topology Display Switch and Status Icons

Switch Icon	Description
	SANbox 5602 Switch ■ Normal operation (Green) ■ Warning–operational with errors (Yellow) ■ Critical–potential failure (Red) ■ Unknown–communication status unknown, unreachable, or unmanageable (Blue)
	Fabric Management Switch ■ Ethernet connection normal (Green) ■ Ethernet connection warning (Yellow) ■ Ethernet connection critical (Red)
	Switch is not manageable with this version of SANsurfer Switch Manager. Use the management application that was shipped with this switch.

3.5.2
Displaying the Event Browser

The Event Browser displays a list of events generated by the switches in the fabric and the SANsurfer Switch Manager application. Events that are generated by the SANsurfer Switch Manager application are not saved on the switch, but can be saved to a file during the SANsurfer Switch Manager session.

Entries in the Event Browser shown in Figure 3-11, are formatted by severity, time stamp, source, type, and description. The maximum number of entries allowed in the Event Browser is 10,000. The maximum number of entries allowed on a switch is 1200. Once the maximum is reached, the event list wraps and the oldest events are discarded and replaced with the new events. Event entries from the switch, use the switch time stamp, while event entries generated by the application have a workstation time stamp. You can filter, sort, and export the contents of the Event Browser to a file. The Event Browser begins recording when enabled and SANsurfer Switch Manager is running.

If the Event Browser is enabled using the Preferences dialog, the next time SANsurfer Switch Manager is started all events from the switch log will be displayed. If the Event Browser is disabled when SANsurfer Switch Manager is started and later enabled, only those events from the time the Event Browser was enabled and forward will be displayed.

To display the Event Browser, open the Fabric menu and select **Show Event Browser**, or click the **Events** button on the tool bar. If the **Show Event Browser** selection or the **Events** button is grayed-out, you must first enable the **Events Browser** preference. Refer to ”Setting SANsurfer Switch Manager Preferences” on page 2-16.

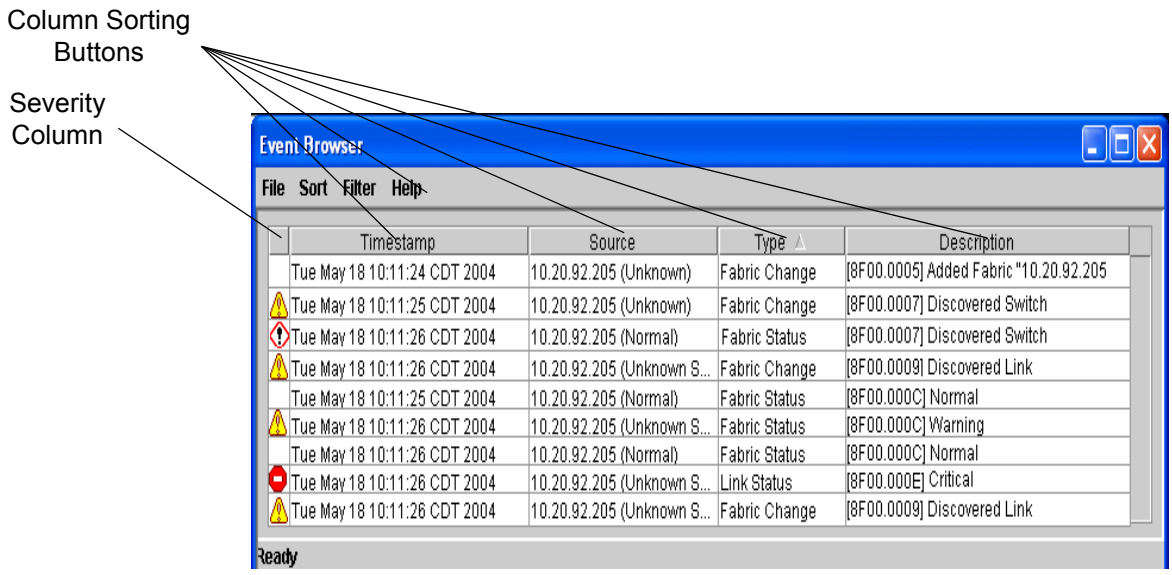


Figure 3-11. Events Browser

Severity is indicated in the severity column using icons as described in Table 3-2.

Table 3-2. Severity Levels

Severity Icon	Description
	Alarm – An Alarm is a "serviceable event". This means that attention by the user or field service is required. Alarms are posted asynchronously to the screen and cannot be turned off. If the alarm denotes that a system error has occurred the customer and/or field representative will generally be directed to provide a "show support" capture of the switch.
	Critical event – An event that indicates a potential failure. Critical log messages are events that warrant notice by the user. By default, these log messages will be posted to the screen. Critical log messages do not have alarm status as they require no immediate attention from a user or service representative.
	Warning event – An event that indicates errors or other conditions that may require attention to maintain maximum performance. Warning messages will not be posted to the screen unless the log is configured to do so. Warning messages are not disruptive and, therefore, do not meet the criteria of Critical. The user need not be informed asynchronously
No icon	Informative – An unclassified event that provides supporting information.

Note:

- Events (Alarms, Critical, Warning, and Informative) generated by the application are not saved on the switch. They are permanently discarded when you close a SANsurfer Switch Manager session, but you can save these events to a file on the workstation before you close SANsurfer Switch Manager and read it later with a text editor or browser.
- Events generated by the switch are stored on switch, and will be retrieved when the application is restarted. Some alarms are configurable. Refer to ”Configuring Port Threshold Alarms” on page 4-14.

3.5.2.1

Filtering the Event Browser

Filtering the Event Browser enables you to display only those events that are of interest based on the event severity, timestamp, source, type, and description. To filter the Event Browser, open the Filter menu and select **Filter Entries**. This opens the Filter Events dialog shown in Figure 3-12. The Event Browser displays those events that meet all of the criteria in the Filter Events dialog. If the filtering criteria is cleared or changed, then all the events that were previously hidden that satisfy the new criteria will be shown.

You can filter the event browser in the following ways:

- Severity – Check one or more of the corresponding check boxes to display alarm events, critical events, warning events, or informative events.
- Date/Time – Check one or both of the From: and To: check boxes. Enter the bounding timestamps (MM/dd/yy hh:mm:ss aa) to display only those events that fall within those times. ("aa" indicates AM or PM.) The current year (yy) can be entered as either 2 or 4 digits. For example, 12/12/03 will be interpreted December 12, 2003.
- Text – Check one or more of the corresponding check boxes and enter a text string (case sensitive) for event source, type, and description. The Event Browser displays only those events that satisfy all of the search specifications for the Source, Type, and Description text.

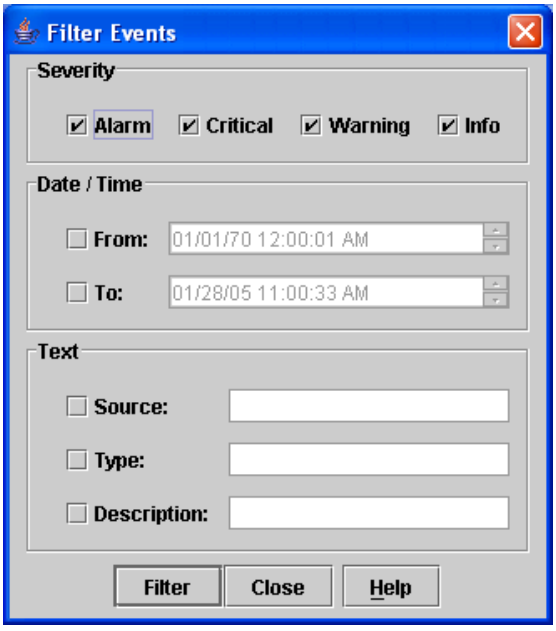


Figure 3-12. Filter Events Dialog

3.5.2.2

Sorting the Event Browser

Sorting the Event Browser enables you to display the events in alphanumeric order based on the event severity, timestamp, source, type, or description. Initially, the Event Browser is sorted in ascending order by timestamp. To sort the Event Browser, click the **Severity**, **Timestamp**, **Source**, **Type**, or **Description** column buttons. You can also open the Sort menu and select **By Severity**, **By Timestamp**, **By Source**, **By Type**, or **By Description**. Successive sort operations of the same type alternate between ascending and descending order.

3.5.2.3

Saving the Event Browser to a File

You can save the displayed Event Browser entries to a file. Filtering affects the save operation, because only displayed events are saved. To save the Event Browser to a file, do the following:

1. Filter and sort the Event Browser to obtain the desired display.
2. Open the File menu and select **Save As**.
3. Select a folder and enter a file name in which to save the event log and click the **Save** button. The file can be saved in XML, CSV, or text format. XML files can be opened with an internet browser or text editor. CSV files can be opened with most spreadsheet applications.

3.5.3
Devices Data Window

The Devices data window displays information about devices (hosts and storage targets) connected to the switch. Click the **Devices** tab below the data window to display device information for all devices that are logged into the selected fabric. To narrow the display to devices that are logged into specific switches, select one or more switches in the fabric tree or the topology display. Table 3-3 describes the entries in the Devices data window. Refer to ”Exporting Device Information to a File” on page 3-36 for exporting device information.

Table 3-3. Devices Data Window Entries

Entry	Description
Port WWN	Port world wide name
Nickname	Device port nickname. To create a new nickname or edit an existing nickname, double-click the cell and enter a nickname in the Edit Nickname dialog. Refer to ”Managing Device Port Nicknames” on page 3-36 for more information.
Details	Click the **(i)** to display additional detail about the device. Refer to ”Displaying Detailed Device Information” on page 3-35.
FC Address	Fibre Channel address
Switch	Switch name
Port	Switch port number
Target/Initiator	Device type: target or initiator
Vendor	Host Bus Adapter/Device Vendor
Host Name	Name of host
Active Zones	The active zone to which the device belongs
Row #	Number of port as displayed in the faceplate display

3.5.4
Active Zone Set Data Window

The Active Zoneset data window displays the zone membership for the active zone set that resides on the fabric management switch. The active zone set is the same on all switches in the fabric – you can confirm this by adding a fabric through another switch and comparing Active Zone Set displays.

To open the Active Zoneset data window, click the **Active Zoneset** tab below the data window in the topology display. Refer to ”Configured Zonesets Data Window” on page 4-13 for information about the zone set definitions on a particular switch. Refer to ”Zoning a Fabric” on page 3-38 for more information about zone sets and zones.

The Active Zoneset data window, shown in Figure 3-13, uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its member ports/devices.
- Ports/devices that are zoned by WWN or FC address, but no longer part of the fabric, are grayed-out.

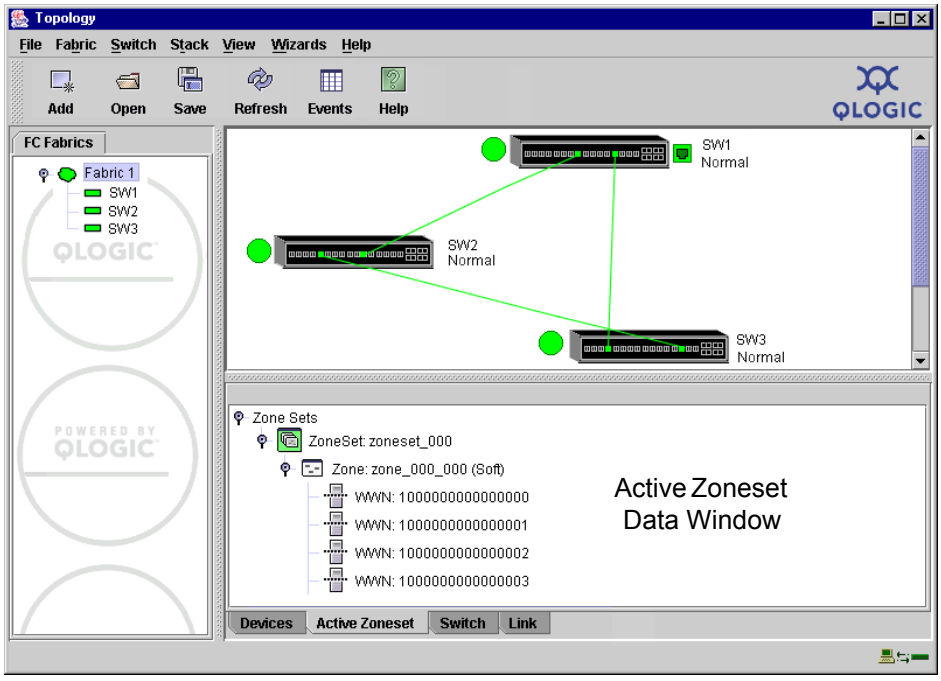


Figure 3-13. Active Zone Set Data Window

3.5.4.1
Link Data Window

The Link data window displays information about all switch links in the fabric or selected links. This information includes the switch name, the port number at the end of each link, and the link status icons. To open the Link data window, click the **Link** tab below the data window in the topology display.

3.6
Working with Device Information and Nicknames

SANsurfer Switch Manager enables you to do the following:

- Displaying Detailed Device Information
- Exporting Device Information to a File
- Managing Device Port Nicknames

3.6.1
Displaying Detailed Device Information

In addition to the information that is available in the Devices data window, you can click the **(i)** in the Details column to display more information shown in Figure 3-14.

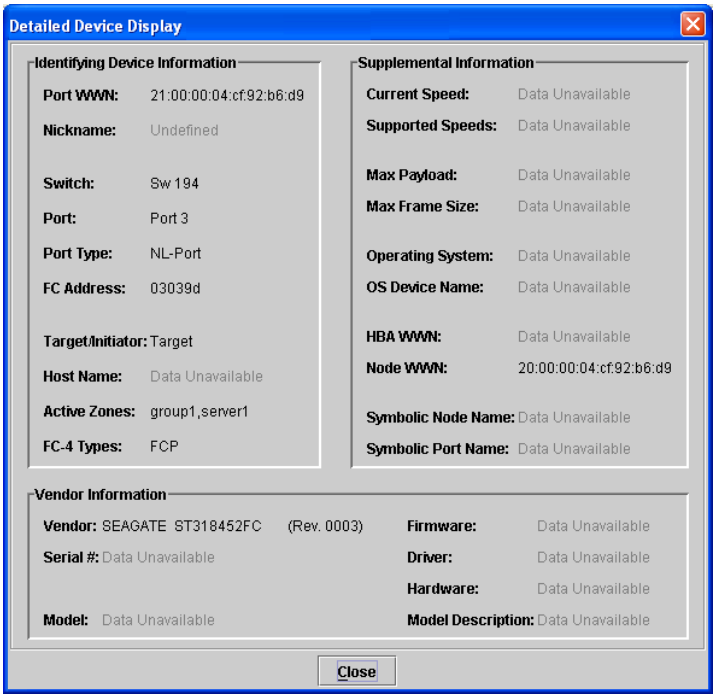


Figure 3-14. Detailed Devices Display Dialog

3.6.2
Exporting Device Information to a File

To save device information to a file, open the topology display and do the following:

1. Select one or more switches. If no switches are selected, Devices information is gathered for all switches.
2. Open the Switch menu and select **Export Devices Information**.
3. In the Save dialog, enter a file name. Select the extension for the type of output file (CSV or text format) to be saved. CSV files can be opened with Microsoft Excel or most spreadsheet applications.
4. Click the **Save** button.

3.6.3
Managing Device Port Nicknames

You can assign a nickname to a device port World Wide Name. A nickname is a user-definable, meaningful name that can be used in place of the World Wide Name. Assigning a nickname makes it easier to recognize device ports when zoning your fabric or when viewing the Devices data window.

SANsurfer Switch Manager maintains nicknames in Nicknames.xml, which is found in your working directory. In addition to creating, editing, and deleting nicknames, you can also export the nicknames to a file, which can then be imported into the Nicknames.xml file on other workstations.

3.6.3.1
Creating a Nickname

To create a device port nickname, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames dialog.
2. Choose one of the following methods to enter a nickname. A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA-zZ][0-9] and special symbols [$ _ - ^].
   - Click on a device in the table. Open the Edit menu and select **Create Nickname** to open the Add Nickname dialog. In the Add Nickname dialog, enter a nickname and WWN and click the **OK** button.
   - Double-click a cell in the **Nicknames** column, and enter a new nickname in the text field. Click the **Save** button to save the changes and exit the Nicknames dialog.

You can also create a nickname by double clicking a cell in the Nickname column of the Devices data window. Refer to ”Devices Data Window” on page 3-33.

3.6.3.2
Editing a Nickname

A nickname must start with a letter and can have up to 64 characters. Valid characters include alphanumeric characters [aA-zZ][0-9] and special symbols [$ _ - ^]. You can access the Edit Nicknames dialog two ways. Choose one of the following methods to edit a nickname. Click the **OK** button to save the changes.

- In the topology or faceplate display, open the File menu and select **Nicknames** to open the Nicknames dialog. The device entries are listed in table format.
  - Click on a device entry in the table. Open the Edit menu and select **Edit Nickname** to open the Edit Nicknames dialog. Edit the nickname in the text field. Click the **OK** button to save the changes.
  - Double-click a cell in the **Nicknames** or **WWN** columns, and edit the nickname in the text field. Click the **OK** button to save the changes.
- In the topology or faceplate display, click the Devices tab to display the Devices data window. Double-click a cell in the Nickname column to open the Edit Nickname dialog. Edit the nickname in the text field. Refer to ”Devices Data Window” on page 3-33.

3.6.3.3
Deleting a Nickname

To delete a device port nickname, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames dialog.
2. Click a device in the table. Open the Edit menu and select **Delete Nickname**.

3.6.3.4
Exporting Nicknames to a File

You can save nicknames to a file. This is useful for distributing nicknames to other management workstations. To save nicknames to an XML file, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames dialog.
2. Open the File menu in the Nicknames dialog, and select **Export**.
3. Enter a name for the XML nickname file in the Save dialog and click **Save**.

3.6.3.5 Importing a Nicknames File

Importing a nicknames file copies its contents into and replaces the contents of the Nicknames.xml file which is used by SANsurfer Switch Manager. To import a nickname file, do the following:

1. Open the File menu and select **Nicknames** to open the Nicknames dialog.
2. Open the File menu in the Nicknames dialog, and select **Import**.
3. Select an XML nickname file in the Open dialog and click **Open**. When prompted to overwrite existing nicknames, click **Yes**.

3.7 Zoning a Fabric

Zoning enables you to divide the ports and devices of the fabric into zones for more efficient and secure communication among functionally grouped nodes. This subsection addresses the following topics:

- Zoning Concepts
- Using the Zoning Wizard
- Managing the Zoning Database
- Managing Zone Sets
- Managing Zones
- Managing Aliases
- Merging Fabrics and Zoning

3.7.1 Zoning Concepts

The following zoning concepts provide some context for the zoning tasks described in this section:

- Zones
- Aliases
- Zone Sets
- Zoning Database

3.7.1.1 Zones

A zone is a named group of ports or devices that can communicate with each other. Devices within a zone can only communicate with other devices in the same zone. A device may participate in more than one zone.

Membership in a zone can be defined by switch domain ID and port number, device Fibre Channel address (FCID), or device World Wide Name (WWN).

- WWN entries define zone membership by the World Wide Name of the attached device. With this membership method, you can move WWN member devices to different switch ports in different zones without having to edit the member entry as you would with a domain ID/port number member. Furthermore, unlike FCID members, WWN zone members are not affected by changes in the fabric that could change the Fibre Channel address of an attached device.
- FCID entries define zone membership by the Fibre Channel address of the attached device. With this membership method you can replace a device on the same port without having to edit the member entry as you would with a WWN member.
- Domain ID/Port number entries define zone membership by switch domain ID and port number. All devices attached to the specified port become members of the zone. The specified port must be an F_Port or an FL_Port.

Two types of zones are supported:

- Soft zone
- Hard zone - Access Control List (domain/port member only or it will revert back to a soft zone when activated)

3.7.1.1.1 Soft Zones

Soft zoning divides the fabric for purposes of controlling discovery. Devices within the same soft zone automatically discover and communicate freely with all other members of the same zone. The soft zone boundary is not secure; traffic across soft zones can occur if addressed correctly. Soft zones that include members from multiple switches need not include the ports of the inter-switch links. Soft zone boundaries yield to ACL zone boundaries. Soft zones can overlap; that is, a device can participate in more than one soft zone. Zone membership can be defined by Fibre Channel address, domain ID and port number, World Wide Name, or a combination. Soft zoning supports all port types.

3.7.1.1.2
Access Control List Hard Zones

Access Control List (ACL) zoning divides the fabric for purposes of controlling discovery and inbound traffic. ACL zoning is a type of hard zoning that is hardware enforced. This type of zoning is useful for controlling access to certain devices without totally isolating them from the fabric. Devices can communicate with each other and transmit outside the ACL zone, but cannot receive inbound traffic from outside the zone. The ACL zone boundary is secure against inbound traffic. ACL zones can overlap; that is, a port can be a member of more than one ACL zone. ACL zones that include members from multiple switches need not include the ports of the inter-switch links. ACL zone boundaries supersede soft zone boundaries. Membership can be defined only by domain ID and port number. ACL zoning supports all port types. You can have domain/port member in a configured ACL zone, but it will be converted to a soft zone when activated.

3.7.1.2
Aliases

To make it easier to add a group of ports or devices to one or more zones, you can create an alias. An alias is a named set of ports or devices that are grouped together for convenience. Unlike zones, aliases impose no communication restrictions between its members. You can add an alias to one or more zones. However, you cannot add a zone to an alias, nor can an alias be a member of another alias.

3.7.1.3
Zone Sets

A zone set is a named group of zones. A zone can be a member of more than one zone set. Each switch in the fabric maintains its own zoning database containing one or more zone sets. This zoning database resides in non-volatile or permanent memory and is therefore retained after a reset. Refer to ”Configured Zonesets Data Window” on page 4-13 for information about displaying the zoning database.

The orphan zone set is created by the application automatically to hold the zones which are not in any set. The orphan zone set cannot be removed and is not saved on the switch.

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. (However, the contents of the aliases are distributed.) This zone set is known as the active zone set. Refer to ”Active Zone Set Data Window” on page 3-34 for information about displaying the active zone set.

3.7.1.4

Zoning Database

Each switch has its own zoning database. The zoning database is made up of all aliases, zones, and zone sets that have been created on the switch or received from other switches. The switch maintains two copies of the inactive zoning database: one copy is maintained in temporary memory for editing purposes; the second copy is maintained in permanent memory. Zoning database edits are made on an individual switch basis and are not propagated to other switches in the fabric when saved.

There are two configuration parameters that affect the zoning database: Interop Auto Save and Default Visibility. The Auto Save parameter determines whether changes to the active zone set that a switch receives from another switch in the fabric will be saved to permanent memory on that switch. The Default Visibility parameter permits or prohibits communication among ports/devices when there is no active zone set. Refer to ”Configuring the Zoning Database” on page 3-46 for information about zoning configuration.

The following zoning limits will be enforced during the configuration of zoning and during a zoning database merge:

- **MaxZoneSets is 256.** The maximum number of zone sets that can be configured on the switch.
- **MaxZones is 2000**. The maximum number of zones that can be configured on the switch.
- **MaxAliases is 2500**. The maximum number of aliases that can be configured on the switch.
- **MaxTotalMembers is 10,000**. The maximum number of total zone and alias members that can be configured on the switch. Aliases are considered zone members since they can be added to a zone just like a normal zone member.
- **MaxZonesInZoneSets is 2000**. The maximum number of zone linkages to zonesets that can be configured on the switch. Every time a zone is added to a zoneset this constitutes a linkage.
- **MaxMembersPerZone is 2000**. The maximum number of zone members that can be added to any zone on the switch. Aliases are considered zone members when added to a zone.
- **MaxMembersPerAlias is 2000**. The maximum number of zone members that can be added to any alias on the switch.

3.7.2
Using the Zoning Wizard

The Zoning Wizard is a series of dialogs that leads you through the process of zoning a fabric. To open the Zoning Wizard, open the Wizards menu in the faceplate display, and select **Zoning Wizard**.

The Zoning Wizard helps you with the two most typical reasons for zoning:

- Zoning Windows servers storage
- Assign storage to servers

To solve these problems, there must be at least one target and at least one initiator in the name server. Windows servers do not share devices well, but sometimes they must share devices, such as a tape drive. The wizard helps you define which devices are sharable and which ones are not. Once a device is in a Windows group, it can no longer be in any other group.

3.7.3
Managing the Zoning Database

Managing the zoning database consists of the following:

- Editing the Zoning Database
- Configuring the Zoning Database
- Saving the Zoning Database to a File
- Restoring the Zoning Database from a File
- Restoring the Default Zoning Database
- Removing All Zoning Definitions

3.7.3.1

Editing the Zoning Database

To edit the zoning database for a particular switch, open the Zoning menu from the faceplate display and select **Edit Zoning** to open the Edit Zoning dialog shown in Figure 3-15. Changes can only be made to inactive zone sets, which are stored in flash (non-volatile) memory and retained after resetting a switch.

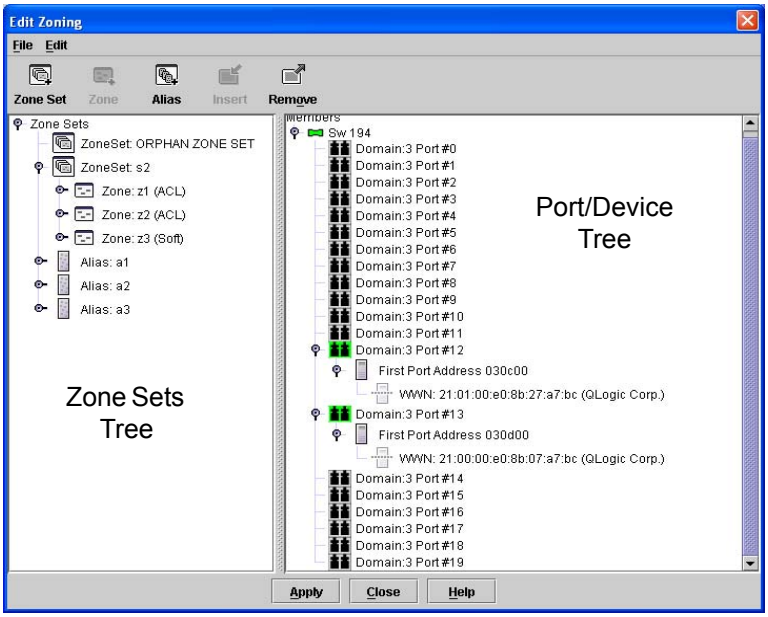


Figure 3-15. Edit Zoning Dialog

To apply zoning to a fabric, choose a zone set and activate it. When you activate a zone set, the switch distributes that zone set and its zones, excluding aliases, to every switch in the fabric. This zone set is known as the active zone set.

You can not edit an active zone set on a switch. You must configure an inactive zone set to your needs and then activate that updated zone set to apply the changes to the fabric. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric. However, in addition to the merged active zone set, each switch maintains its own original zone set in its zoning database. Only one zone set can be active at one time.

Note: If the Interop Auto Save parameter is enabled on the Zoning Configuration dialog, then every time the active zone set changes, the switch will copy it into an inactive zone set stored on the switch. You can edit this copy of the active zone set stored on the switch, and activate the updated copy to conveniently apply the changes to the active zone set. The edited copy then becomes the active zone set.

The Edit Zoning dialog has a Zone Sets tree on the left and a Port/Device (or members) tree on the right. Both trees use display conventions similar to the fabric tree for expanding and contracting zone sets, zones, and ports. An expanded port shows the port Fibre Channel address; an expanded address shows the port World Wide Name. You can select zone sets, zones, and ports in the following ways:

- Click a zone, zone set, or port icon.
- Right-click to select a zone set or zone, and open the corresponding popup menu.
- Hold down the Shift key while clicking several consecutive icons.
- Hold down the Control key while clicking several non-consecutive icons.

Using tool bar buttons, popup menus, or a drag-and-drop method, you can create and manage zone sets and zones in the zoning database. Table 3-4 describes the zoning tool bar operations.

Use the Edit Zoning dialog to define zoning changes, and click the **Apply** button to open the Error Check dialog. Click the **Error Check** button to have SANsurfer Switch Manager check for zoning conflicts, such as empty zones, aliases, or zone sets, and ACL zones with non-domain ID/port number membership. Click the **Save Zoning** button to implement the changes. Click the **Close** button to close the Error Check dialog. On the Edit Zoning dialog, click the **Close** button to close the Edit Zoning dialog.

Table 3-4. Edit Zoning Dialog Tool Bar Buttons and Icons

Tool Bar Button	Description
	Create Zone Set button - create a new zone set
	Create Zone button - create a new zone
	Create Alias button - create another name for a set of objects
	Add Member button - add selected port/device to a zone
	Remove Member button - delete the selected zone from a zone set, or delete the selected port/device from a zone
	Switch port icon – not logged in
	Switch port icon – logged in
	NL_Port (loop) device icon – logged in to fabric
	NL_Port (loop) device icon – not logged in to fabric
	N_Port device icon – logged in to fabric
	N_Port device icon – not logged in to fabric

3.7.3.2
Configuring the Zoning Database

Use the Zoning Config dialog to change the Interop Auto Save, Default Visibility, and Discard Inactive parameters. In the faceplate display, open the Zoning menu and select **Edit Zoning Config** to open the Zoning Config dialog shown in Figure 3-16. After making changes, click the **OK** button to put the new values into effect.

Figure 3-16. Zoning Config Dialog

3.7.3.2.1
Interop Auto Save

The Interop Auto Save parameter determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to the zoning database on that switch. Changes are saved when an updated zone set is activated. Zoning changes are always saved to temporary memory. However, if Interop Auto Save is enabled, the switch firmware saves changes to the active zone set in temporary memory and to the zoning database. If Interop Auto Save is disabled, changes to the active zone set are stored only in temporary memory which is cleared when the switch is reset.

Note: Disabling the Interop Auto Save parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Interop Auto Save parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Interop Auto Save parameter should be enabled in a production environment.

3.7.3.2.2

Default Visibility

Default visibility determines the level of communication that is permitted among ports/devices when there is no active zone set. The default visibility parameter can be set differently on each switch. When default visibility is enabled (ALL) on a switch, all ports/devices on the switch can communicate with all ports/devices on switches that also have default visibility enabled. When Default Visibility is disabled (NONE), none of the ports/devices on that switch can communicate with any other port/device in the fabric.

3.7.3.2.3

Discard Inactive

The Discard Inactive parameter automatically removes inactive zones and zone sets when a zoneset is activated or deactivated from a remote switch.

3.7.3.3

Saving the Zoning Database to a File

You can save the zoning database to an XML file. You can later reload this zoning database on the same switch or another switch. To save a zoning database to a file, do the following:

1. In the faceplate display, open the Zoning menu, and select **Edit Zoning**.
2. In the Edit Zoning dialog, open the File menu and select **Save As**.
3. In the Save dialog, enter a file name for the database file.
4. Click the **Save** button to save the zoning file.

3.7.3.4

Restoring the Zoning Database from a File

CAUTION! Restoring the zoning database from a file will replace the current zoning database on the switch.

Do the following to restore the zoning database from a file to a switch:

1. In the faceplate display, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning window.
2. Open the File menu and select **Open File**. A popup window will prompt you to select an XML zoning database file.
3. Select a file and click **Open**.

3.7.3.5

Restoring the Default Zoning Database

Restoring the default zoning clears the switch of all zoning definitions.

CAUTION! This command will deactivate the active zone set.

To restore the default zoning for a switch:

1. In the faceplate display, open the Zoning menu and select **Restore Default Zoning**.
2. Click the **OK** button to confirm that you want to restore default zoning and save changes to the zoning database.

3.7.3.6

Removing All Zoning Definitions

To clear all zone and zone set definitions from the zoning database, choose one of the following:

- Open the Edit menu and select **Clear Zoning**. In the Removes All dialog, click the **Yes** button to confirm that you want to delete all zones and zone sets.
- Right-click the Zone Sets heading at the top of the Zone Sets tree, and select **Clear Zoning** from the popup menu. Click the **Yes** button to confirm that you want to delete all zone sets and zones.

3.7.4
Managing Zone Sets

Zoning a fabric involves creating a zone set, creating zones as zone set members, then adding devices as zone members. The zoning database supports multiple zone sets to serve the different security and access needs of your storage area network, but only one zone set can be active at one time. Managing zone sets consists of the following tasks:

- Creating a Zone Set
- Activating and Deactivating a Zone Set
- Copying a Zone to a Zone Set
- Removing a Zone from a Zone Set or from All Zone Sets
- Removing a Zone Set

Note: Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

3.7.4.1
Creating a Zone Set

To create a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Open the Edit menu, and select **Create Zone Set** to open the Create Zone Set dialog.
3. Enter a name for the zone set, and click the **OK** button. The new zone set name is displayed in the Zone Sets dialog. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, -, ^, and $.

4. To create new zones in a zone set, do one of the following:
   - Right-click a zone set and select **Create A Zone** from the popup menu. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog.
   - Select a zone set in the zone sets tree, and click the **Zone** button in the Zoning toolbar. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog.
   - Copy an existing zone by dragging a zone into the new zone set. Refer to ”Copying a Zone to a Zone Set” on page 3-50.
5. Click the **Apply** button to save changes to the zoning database.

3.7.4.2 Activating and Deactivating a Zone Set

You must activate a zone set to apply its zoning definitions to the fabric. Only one zone set can be active at one time. When you activate a zone set, the switch distributes that zone set to the temporary zoning database on every switch in the fabric.

The purpose of the deactivate function is to suspend all fabric zoning which results in free communication fabric wide or no communication depending on the default visibility setting. Refer to ”Default Visibility” on page 3-47 for more information. It is not necessary to deactivate the active zone set before activating a new one.

- To activate a zone set, open the Zoning menu and select **Activate Zone Set** to open the Activate Zone Set dialog. Select a zone set from the Select Zone Set pull-down menu, and click the **Activate** button.
- To deactivate the active zone set, open the Zoning menu, select **Deactivate Zone Set**. Acknowledge the warning about traffic disruption, and click the **Yes** button to confirm that you want to deactivate the active zone set.

3.7.4.3 Copying a Zone to a Zone Set

To copy an existing zone and its membership from one zone set to another, select the zone and drag it to the chosen zone set. Click the **Apply** button to save changes to the zoning database.

3.7.4.4

Removing a Zone from a Zone Set or from All Zone Sets

You can remove a zone from a zone set or from all zone sets in the database.

1. In the faceplate display, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the Zone Sets tree, select the zone(s) to be removed.
3. Open the Edit menu, and select **Remove** to remove the zone from the zone set, or select **Remove from All Zones** to remove the zone from all zone sets.
4. Click the **Apply** button to save changes to the zoning database.

Alternatively, you may use shortcut menus to remove a zone from a zone set or from all zone sets in the database.

3.7.4.5

Removing a Zone Set

Removing a zone set from the database affects the member zones in the following ways.

- Member zones that are members of other zone sets are not affected.
- The orphan zone set is created by the application automatically to hold the zones which are not in any set. The orphan zone set cannot be removed and is not saved on the switch.

To delete a zone set from the database, do the following:

1. In the faceplate display, open the Zoning menu and select **Edit Zoning** to open the Edit Zoning dialog.
2. In the Zone Sets tree, select the zone set to be removed.
3. Open the Edit menu, and select **Remove** to remove the zone set.
4. Click the **Apply** button to save changes to the zoning database.

Alternatively, you may use shortcut menus to remove a zone set from the database. However, the orphan zone set can not be removed.

3.7.5
Managing Zones

Managing zones involves the following:

- Creating a Zone in a Zone Set
- Adding Zone Members
- Renaming a Zone or a Zone Set
- Removing a Zone Member
- Removing a Zone from a Zone Set
- Removing a Zone from All Zone Sets
- Changing Zone Types

Note: Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

3.7.5.1

Creating a Zone in a Zone Set

When a zone is created, its zone type is soft. To change the zone type to a hard zone, refer to ”Changing Zone Types” on page 3-56 for more information. Refer to ”Zones” on page 3-39 for information on zone types (soft and hard). To create a zone in a zone set, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Select a zone set.
3. Open the Edit menu and select **Create a Zone**.
4. In the Create a Zone dialog, enter a name for the new zone, and click the **OK** button. The new zone name is displayed in the Zone Sets dialog. A zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, ^, $, and -.

   Note: If you enter the name of a zone that already exists in the database, the SANsurfer Switch Manager application will ask if you would like to add that zone and its membership to the zone set.

5. To add switch ports or attached devices to the zone, do one of the following:
   - In the zone set tree, select the zone set. In the graphic window, select the port to add to the zone. Open the Edit menu and select **Add Members**.
   - Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree, and drag it into the zone.
   - Select a port by port number, Fibre Channel address, or World Wide Name in the Port/Device tree. Right-click the zone and select **Add Zone Members** from the popup menu.
6. Click the **Apply** button to save changes to the zoning database.

3.7.5.2

Adding Zone Members

You can zone a port/device by switch domain ID and port number, device port Fibre Channel address, or the device port WWN. Adding a port/device to a zone affects every zone set in which that zone is a member. To add ports/devices to a zone, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following methods to add the port/device:
   - Select a port/device in the Port/Device tree, and drag it into the zone. To select multiple ports/devices, press and hold the Control key while selecting.
   - Select a port/device in the Port/Device tree. To select multiple ports/devices, press the Control key while selecting. Select a zone set in the left pane. Open the Edit menu and select **Add Members**.
   - Select a port/device in the Port/Device tree. To select multiple ports/devices, press the Control key while selecting. Select a zone set in the left pane. Click the **Insert** button.

   If the port/device you want to add is not in the Port/Device tree, you can add it by doing the following:
   a. Right click the selected zone.
   b. Open the Edit menu and select **Create Members**.
   c. Choose the **WWN**, **Domain/Port**, or **First Port Address** radio button.
   d. Enter the hexadecimal value for the port/device according to the radio button selection: 16 digits for a WWN member, 4 digits for a Domain/Port member (DDPP), or a 6-digit Fibre Channel Address for a First Port Address member (DDPPAA) where D=domain ID, P=port number, and A=ALPA.
3. Click the **OK** button to add the member and save the change.

Note: Domain ID conflicts can result in automatic reassignment of switch domain IDs. These reassignments are not reflected in zones that use domain ID/port number pair to define their membership. Be sure to reconfigure zones that are affected by a domain ID change.

3.7.5.3
Renaming a Zone or a Zone Set

To rename a zone, do the following:

1. In the Zone Sets tree of the Edit Zoning dialog, click the zone/zone set to be renamed.
2. Open the Edit menu and select **Rename**.
3. In the Rename Zone/Rename Zone Set dialog, enter a new name for the zone/zone set.
4. Click the **OK** button.

3.7.5.4
Removing a Zone Member

Removing a zone member will affect every zone and zone set in which that zone is a member. To remove a member from a zone:

1. In the Edit Zoning dialog, select the zone member to be removed.
2. Open the Edit menu and select **Remove**.
3. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.7.5.5
Removing a Zone from a Zone Set

The orphan zone set is created by the application automatically to hold the zones which are not in any set. The orphan zone set cannot be removed and is not saved on the switch. To remove a zone from a zone set, do the following:

1. In the Edit Zoning dialog, select the zone to be removed. The selected zone will be removed from that zone set only.
2. Open the Edit menu and select **Remove**.
3. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.7.5.6
Removing a Zone from All Zone Sets

To remove a zone from all zone sets, do the following:

1. In the Edit Zoning dialog, select the zone to be removed.
2. Open the Edit menu and select **Remove Zone from All Sets**.
3. Click the **OK** button to save changes and close the Edit Zoning dialog.

3.7.5.7
Changing Zone Types

To change a zone type, do the following:

1. In the faceplate display, select the switch with the zone type to change.
2. Click the **Zoning** button to open the Edit Zoning dialog.
3. In the Zone Sets tree, select the zone to change.
4. Open the Edit menu and select **Set Zone Type** to open the Set Zone Type dialog.
5. Open the Zone Type pull-down menu and select **Soft** or **ACL**.
   - Soft zoning is the least restrictive type of zoning.
   - ACL zoning is hard zoning and is enforced by hardware and defines access to a given port. ACL zones need not include inter-switch links.

3.7.6
Managing Aliases

An alias is a collection of objects that can be zoned together. An alias is not a zone, and can not have a zone or another alias as a member.

Note: Changes that you make to the zoning database are limited to the managed switch and do not propagate to the rest of the fabric. To distribute changes to configured zone sets fabric wide, you must edit the zoning databases on the individual switches.

You will not see aliases in the active zone set.

3.7.6.1
Creating an Alias

To create an alias, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Open the Edit menu, and select **Create Alias** to open the Create Alias dialog.
3. Enter a name for the alias, and click the **OK** button. The alias name is displayed in the Zone Sets dialog. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -.
4. Click the **OK** button to save the alias name to the zoning database.

3.7.6.2
Adding a Member to an Alias

You can add a port/device to an alias by domain ID and port number, device port Fibre Channel address, or the device port WWN. To add ports/devices to an alias, do the following:

1. Open the Zoning menu, and select **Edit Zoning** to open the Edit Zoning dialog.
2. Choose one of the following methods to add the port/device:
   - Select a port/device in the Port/Device tree, and drag it into the alias. To select multiple ports/devices, press and hold the Control key while selecting.
   - Select a port/device in the Port/Device tree. Click an alias to select multiple ports/devices, press the Control key while selecting. Select an alias. Open the Edit menu and select **Add Members**.
   - Select a port/device in the Port/Device tree. To select multiple ports/devices, press the Control key while selecting. Select an alias. Click the **Insert** button.

   If the port/device you want to add is not in the Port/Device tree, you can add it by doing the following:
   a. Right click the selected alias.
   b. Open the Edit menu and select **Create Members**.
   c. Choose the **WWN**, **Domain/Port**, or **First Port Address** radio button.
   d. Enter the hexadecimal value for the port/device according to the radio button selection: 16 digits for a WWN member, 4 digits for a Domain/Port member (DDPP), or a 6-digit Fibre Channel Address for a First Port Address member (DDPPAA) where D=domain ID, P=port number, and A=ALPA.
3. Click the **OK** button to add the member and save the change.

3.7.6.3
Removing an Alias from All Zones

To remove an alias from all zones, do the following:

1. In the Zone Sets tree in the Edit Zoning dialog, select the alias to be removed.
2. Open the Edit menu, and select **Remove Alias from All Zones**.
3. Click the **Yes** button in the Remove dialog.

3.7.7
Merging Fabrics and Zoning

If you join two fabrics with an inter-switch link, the active zone sets from the two fabrics attempt to merge automatically. The fabrics may consist of a single switch or many switches already connected together. The switches in the two fabrics attempt to create a new active zone set containing the union of each fabric's active zone set. The propagation of zoning information only affects the active zone set, not the configured zone sets, unless Interop Auto Save is turned on.

3.7.7.1
Zone Merge Failure

If a zone merge is unsuccessful, the inter-switch links between the fabrics will isolate due to a zone merge failure, which will generate an alarm. The reason for the E_Port isolation can also be determined by viewing the port information. Refer to ”Port Information Data Window” on page 5-8 and the ”Show Command” on page A-91 (Port keyword).

A zone merge will fail if the two active zone sets have member zones with identical names that differ in membership or type. For example, consider Fabric A and Fabric B each with a soft zone named “ZN1” in its active zone set. Fabric A "ZN1" contains a member specified by Domain ID 1 and Port 1; Fabric B “ZN1” contains a member specified by Domain ID 1 and Port 2. In this case, the merge will fail because the two zones have the same name, but different membership.

3.7.7.2
Zone Merge Failure Recovery

When a zone merge failure occurs, the conflict that caused the failure must be resolved. You can correct a failure due to a zone conflict by deactivating one of the active zone sets or by editing the conflicting zones so that their membership is the same. You can deactivate the active zone set on one fabric if the active zone set on the other fabric accurately defines your zoning needs. If not, you must edit the zone memberships, and reactivate the zone sets. After correcting the zone membership, reset the isolated ports to allow the fabrics to join. Refer to ”Managing Zones” on page 3-52 for information about adding and removing zone members. Refer to ”Resetting a Port” on page 5-15 for information about resetting a port.

Note: If you deactivate the active zone set in one fabric and the Interop Auto Save parameter is enabled, the active zone set from the second fabric will propagate to the first fabric and replace all zones with matching names in the configured zone sets. If the zone sets to merge have the same Zone A that only differ in the type of zone (soft vs. ACL), the zone sets will merge. If this is a two switch fabric, Switch 1 will state that Zone A is soft and Switch 2 will state that Zone A is ACL.

Section 4

Managing Switches

This section describes the following tasks that manage switches in the fabric.

- Managing User Accounts
- Displaying Switch Information
- Configuring Port Threshold Alarms
- Paging a Switch
- Setting the Date/Time and Enabling NTP Client
- Resetting a Switch
- Configuring a Switch
- Managing Switch Stacks
- Archiving a Switch
- Restoring a Switch
- Restoring the Factory Default Configuration
- Downloading a Support File
- Upgrading the Switch Using License Keys
- Installing Firmware
- Displaying Hardware Status

4.1 Managing User Accounts

Only the Admin account can manage user accounts with the User Account Administration dialogs. However, any user can modify their own password. To open the User Account Administration dialogs, open the Switch menu in the faceplate display, and select **User Accounts...**. A user account consists of the following:

- Account name or login
- Password
- Authority level
- Expiration date

Switches come from the factory with the following user accounts:

Table 4-1. Factory User Accounts

Account Name	Password	Admin Authority	Expiration
admin	admin	true	never expires
images	images	false	never expires

The Admin account is the only user that can manage all user accounts with the User Account Administration dialogs. The Admin account can create, remove, or modify user accounts, and change account passwords. The Admin account can also view and modify the switch and its configuration with SANsurfer Switch Manager. The Admin account can not be removed.

Users with Admin authority can view and modify the switch and its configuration using SANsurfer Switch Manager. Users without Admin authority are limited to viewing switch status and configuration.

The Images account is used to exchange files with the switch using FTP. The Images account can not be removed.

Note: If the same user account exists on a switch and its RADIUS server, that user can login with either password, but the authority and account expiration will always come from the switch database.

4.1.1
Creating User Accounts

To create a user account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. This displays the User Account Administration dialog shown in Figure 4-1. A switch can have a maximum of 15 user accounts.

Figure 4-1. User Account Administration Dialog – Add Account

1. To open the User Account Administration dialogs, open the Switch menu in the faceplate display, and select **User Accounts...**.
2. Click the **Add Account** tab to open the Add Account tab page.
3. Enter an account name in the New Account Login field. Account names are limited to 15 characters.
4. If the account is to have the ability to modify switch configurations, check the **Admin Authority Enabled** box.
5. Enter a password in the New Password field and enter it again in the Verify Password field. A password must have a minimum of 8 characters and no more than 20.
6. If this account is to be permanent with no expiration date, click the **Permanent Account** radio button. Otherwise, click the **Account Will Expire** button and enter the number days in which the account will expire.
7. Click the **Add Account** button to add the newly defined account.

4.1.2
Removing a User Account

To remove a user account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. Click the **Remove Account** tab in the dialog to present the display shown in Figure 4-2. Select the account (login) name from the list of accounts at the top of the dialog and click the **Remove Account** button.

Figure 4-2. User Account Administration Dialog – Remove Account

4.1.3
Changing a User Account Password

To change the password for an account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. Click the **Change Password** tab in the dialog to present the display shown in Figure 4-3. Select the account (login) name from the list of accounts at the top of the dialog, then enter the old password, the new password, and verify the new password in the corresponding fields. Click the **Change Password** button. Any user can change their password for their account, but only the Admin account name can change the password for another user's account. If the administrator does not know the user's original password, the administrator must remove the account and add the account.

Figure 4-3. User Account Administration Dialog – Change Password

4.1.4
Modifying a User Account

To modify a user account on a switch, open the Switch menu in the faceplate display and select **User Accounts...**. This displays the User Account Administration dialog shown in Figure 4-4. Click the **Modify Account** tab. Select the account (login) name from the list of accounts at the top of the dialog. Click the Admin authority Enabled check box to grant admin authority to the account name. Click an Account Expiration Date radio button. If the account is not to be permanent, enter the number of days until the account expires. Click the **Modify Account** button to save the changes. Click the **Close** button to close the User Account Administration dialog.

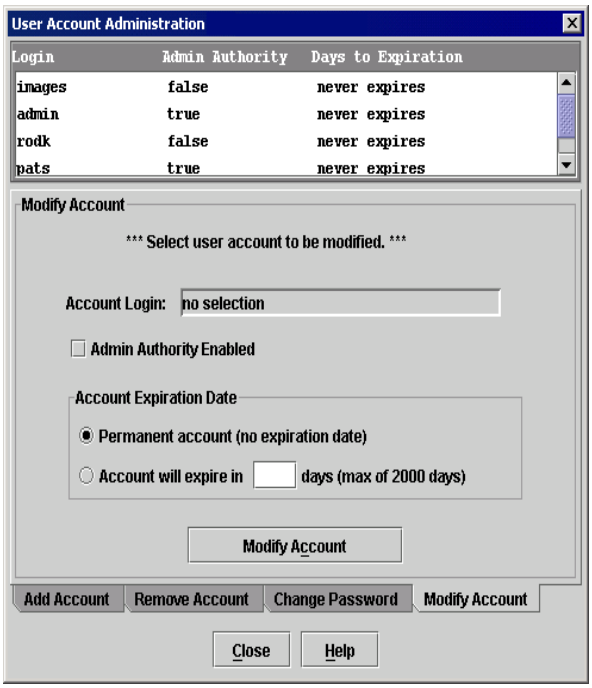


Figure 4-4. User Account Administration Dialog - Modify Account

4.2 Displaying Switch Information

The faceplate display and data windows provide the following switch information:

- Device and HBA information
- Switch specifications and addresses
- Configuration parameters
- Port performance statistics
- Port information
- Configured zone sets

Figure 4-5 shows the faceplate display for the SANbox 5602 switch.

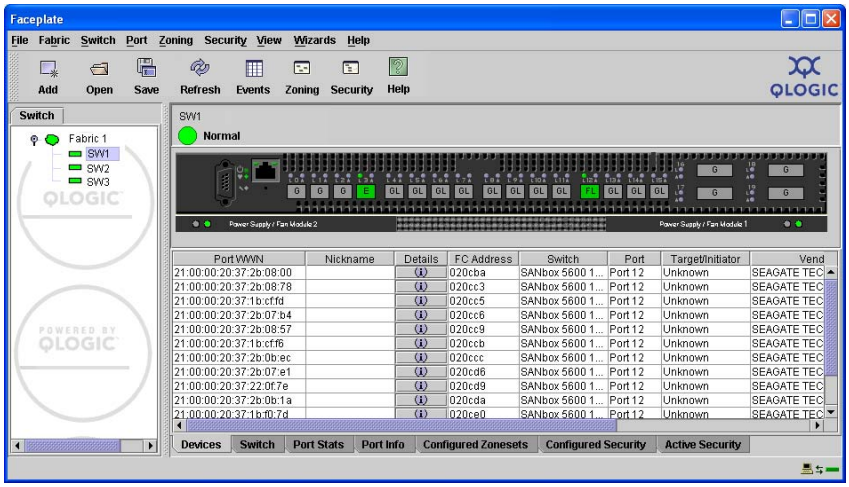

Faceplate
File Fabric Switch Port Zoning Security View Wizards Help
Add Open Save Refresh Events Zoning Security Help
QLOGIC
Switch
Fabric 1
SW1
SW2
SW3
SW1
Normal
Power Supply / Fan Module 2
Power Supply / Fan Module 1
Port WWN Nickname Details FC Address Switch Port Target/Initiator Vend
21:00:00:20:37:2b:08:00 020cba SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:08:78 020cc3 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:1b:cf:fd 020cc5 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:07:b4 020cc6 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:08:57 020cc9 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:1b:cf:f6 020ccb SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:0b:ec 020ccc SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:07:e1 020cd6 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:22:0f:7e 020cd9 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:2b:0b:1a 020cda SANbox 5600 1... Port 12 Unknown SEAGATE TEC
21:00:00:20:37:1b:f0:7d 020ce0 SANbox 5600 1... Port 12 Unknown SEAGATE TEC
Devices Switch Port Stats Port Info Configured Zonesets Configured Security Active Security

Figure 4-5. Faceplate Display - Switch Information

The fabric updates the topology and faceplate displays by forwarding changes in status to the management workstation as they occur. You can allow the fabric to update the switch status, or you can refresh the display at any time. To refresh switch status in the display, do one of the following:

- Click the **Refresh** button.
- Open the View menu and select **Refresh**.
- Press the F5 key.
- Right-click a switch in the topology display and select **Refresh Switch** from the popup menu.
- Right-click in the graphic window of the faceplate display, and select **Refresh Switch** from the popup menu.

4.2.1 Devices Data Window

The Devices data window displays information about devices (hosts and storage targets) connected to the switch. Click the **Devices** tab below the data window to display name server information for all devices that are logged into the selected fabric. To narrow the display to devices that are logged into specific switches, select one or more switches in the fabric tree or the topology display. Refer to ”Devices Data Window” on page 3-33 for a description of the entries in the Devices data window.

4.2.2 Switch Data Window

The Switch data window displays current network and switch information for the selected switches. Refer to ”Configuring a Switch” on page 4-18 for more information about the Switch data window. To open the Switch data window, select one or more switches in the topology display, or open the faceplate display, and click the **Switch** tab below the data window. Table 4-2 describes the Switch data window entries.

Table 4-2. Switch Data Window Entries

Entry	Description
Switch Type	Switch model
First Port Address	Switch Fibre Channel address
World Wide Name	Switch World Wide Name
Serial Number	Number assigned to each chassis. Required for license keys
Reason for Status	Additional status information
User Name	Account name
Login Level	Authority level
Super User	Super user privileges enabled/disabled
UserAuthentication Enabled	Enforcement of account names and authority (always True)
Vendor	Switch manufacturer
Firmware Version	Active firmware version
Inactive Firmware Version	This field does not apply to this switch
Pending Firmware Version	Firmware version that will be activated at the next reset

Table 4-2. Switch Data Window Entries (Continued)

Entry	Description
PROM/Boot Version	PROM boot version
MAC Address	Media Access Control address
IP Address	Internet Protocol address
Subnet Mask	Mask that determines the IP address subnet
Gateway	Gateway address
SNMP Enabled	SNMP enabled or disabled.
Negotiated Domain ID	The domain ID currently being used by the fabric
Configured Domain ID	The domain ID defined by network administrator
Domain ID Lock	Domain ID lock status. Prevents (True) or permits (False) dynamic domain ID reassignment.
Number of Ports	Number of ports activated on the switch.
Operational State	Switch operational state: Online, Offline, Diagnostic, Down
Administrative State	Current switch administrative state
Configured Admin State	Switch administrative state that is stored in the switch configuration
R_A_TOV	Resource allocation timeout value
E_D_TOV	Error detect timeout value
Interop Mode	Zoning merge status. When a zone set is activated on an FC-SW-2 compliant switch, only the active zone set is propagated to all switches in the fabric. When a zone set is activated on a non-FC-SW-2 compliant switch, the active zone set and all inactive zone sets (the entire zoning database) are stored in permanent memory. The Interop Mode setting must be the same on all switches in the fabric, otherwise the inter-switch links will not connect.
Legacy Address Format	Legacy port addressing status. Enabled only for interoperability with non-FC-SW-2 compliant switches.
Interop Auto Save	Zoning auto save status. Saves zoning updates in temporary memory and the zoning database (True) or only in temporary memory (False).

Table 4-2. Switch Data Window Entries (Continued)

Entry	Description
Zoning Default Visibility	Zoning visibility status. Permits (All) or prevents (None) communication between attached devices in the absence of an active zone set.
Security Auto Save	N/A - does not apply to this switch
Security Fabric Binding Enable	N/A - does not apply to this switch
Temperature	Internal switch temperature °C
Fan 1 Status	The status of Fan 1
Fan 2 Status	The status of Fan 2
Fan 3 Status	N/A - does not apply to this switch
Power Supply 1 Status	Power supply 1 status
Power Supply 2 Status	Power supply 2 status
Beacon Status	Beacon status. Switch LEDs are blinking (On) or not (off).
Broadcast Support	Broadcast support status. Broadcast support is enabled or disabled (default).
In-band Enabled	In-band management status. Permits (True) or prevents (False) a switch from being managed over an ISL.
Temperature Failure Port Shutdown	Non-configurable (always enabled for this switch). All ports are downed when the switch temperature exceeds the Failure Temperature.
Warning Temperature	Non-configurable temperature threshold (65° Celsius) above which a warning condition alarm is generated.
Failure Temperature	Non-configurable temperature threshold (70° Celsius) above which a failure condition alarm is generated.
NTP Client Enabled	Enabled or disabled. Allows for switches to synchronize their time a centralized server.
NTP Server Address	The IP address of the centralized NTP server. Ethernet connection to NTP server is required.
FDMI HBA Entry Limit	Maximum number of HBAs that can be registered with a switch.

Table 4-2. Switch Data Window Entries (Continued)

Entry	Description
FDMI Enable	Fabric Device Management Interface status. If enabled, device information can be obtained, managed, and saved through the fabric using Name Service Management Server functions. SANsurfer Switch Manager will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. Refer to ”Displaying Detailed Device Information” on page 3-35 for information about displaying FDMI information.
Number of Donor Groups	Total number of donor port groups. A donor group is a set of (1-Gbps/2-Gbps only) ports on a switch that can donate buffer credits to each other.
Embedded GUI	SANsurfer Switch Manager web applet status. Enables or disables the web applet on the switch.
Inactivity Timeout	Number of minutes the switch waits before terminating an idle command line interface session. Zero (0) disables the time out threshold.
GUI Mgmt Enabled	Switch management application status. If disabled, the switch cannot be managed using the application.
Telnet Enabled	Telnet client status
SSH Enabled	Secure Shell status. If enabled, an encrypted data path is provided for command line interface sessions.
SSL Enabled	Secure Sockets Layer status. If enabled, encryption for switch management application and CIM sessions is provided.
CIM Enabled	Common Information Model status. The CIM agent is based on the SNIA Storage Management Initiative Specification (SMI-S), which is the standard for SAN management in a heterogeneous environment.
FTP Enabled	FTP status
Management Server Enabled	Management server status.

4.2.3
Port Statistics Data Window

The Port Statistics data window displays port performance data for the selected ports. To open the Port Statistics data window, click the **Port Stats** tab below the data window in the faceplate display. Refer to Table 5-6 for a description of the Port Statistics data window entries.

The Statistics pull-down menu is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the pull-down menu. Open the pull-down menu and select **Absolute** to view the total count of statistics since the last switch reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. Click the **Clear Baseline** button to set the current baseline.

4.2.4
Port Information Data Window

The Port Information data window displays port detail information for the selected ports. To open the Port Statistics data window, click the **Port Info** tab below the data window in the faceplate display. Refer to Table 5-6 for a description of the Port Information data window entries.

4.2.5
Configured Zonesets Data Window

The Configured Zonesets data window displays all zone sets, zones, aliases, and zone membership in the zoning database, as shown in Figure 4-6. To open the Configured Zonesets data window, click the **Configured Zonesets** tab below the data window in the faceplate display. To view the active zone set in the Active Zonesets data window, open the topology display and click the **Active Zonesets** data window tab.

The Configured Zonesets data window uses display conventions for expanding and contracting entries that are similar to the fabric tree. An entry handle located to the left of an entry in the tree indicates that the entry can be expanded. Click this handle or double-click the following entries to expand or collapse them:

- A zone set entry expands to show its member zones.
- A zone entry expands to show its members by device port World Wide Name, or device port Fibre Channel address.
- The alias entry expands to show its entries.

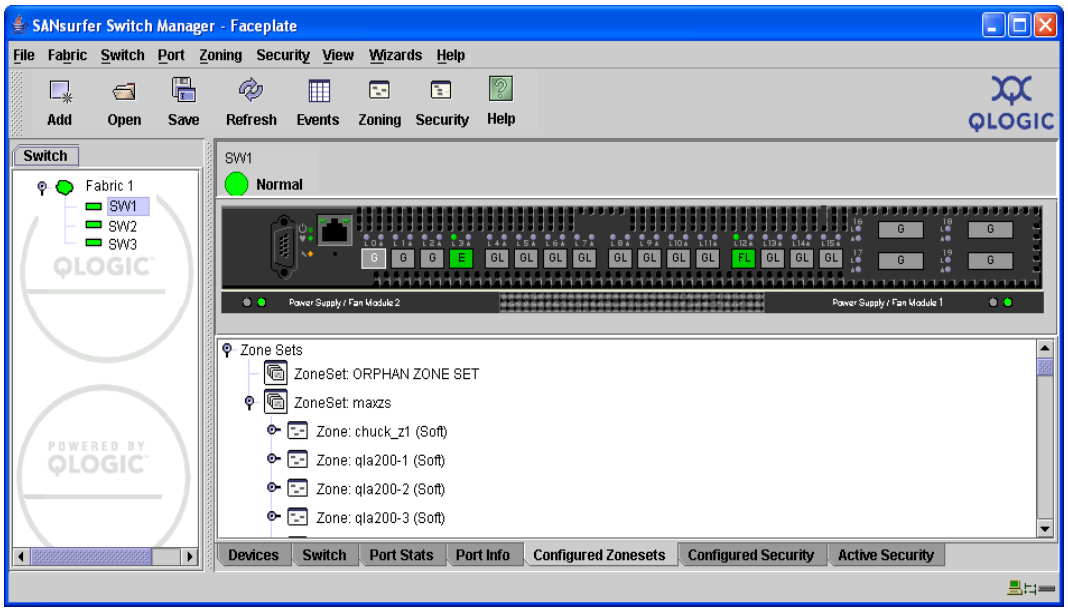


Figure 4-6. Configured Zonesets Data Window

4.3
Configuring Port Threshold Alarms

You can configure the switch to generate alarms for selected events. Configuring an alarm involves choosing an event type, rising and falling triggers, a sample window, and finally enabling or disabling the alarm. To configure port threshold alarms, do the following:

1. In the faceplate display, open the Switch menu and select **Port Threshold Alarm Configuration**. The Port Threshold Alarm Configuration dialog shown in Figure 4-7 prompts you to enable or disable all alarms, select an event, set triggers, set a sample window and enable or disable an individual alarm.

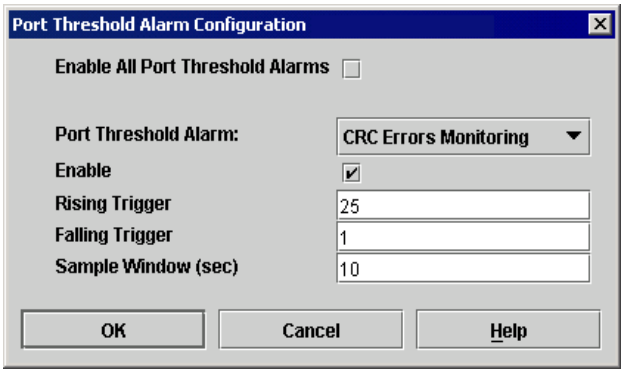


Figure 4-7. Port Threshold Alarm Configuration Dialog

2. Check the **Enable All Port Threshold Alarms** check box to enable monitoring for all the individual alarm types that are enabled. The **Enable All Port Threshold Alarms** check box is the master control for the individual alarms. For example, the switch will monitor CRC errors only if both the **CRC Error Monitoring** box and the **Enable All Port Threshold Alarms** check box are checked.
3. Select an event type from the Port Threshold Alarm pull-down menu. Choose from the following options:
   - CRC error monitoring
   - Decode error monitoring
   - ISL monitoring
   - Login monitoring
   - Logout monitoring
   - Loss of signal monitoring
4. Check the **Enable** box to make the alarm eligible for use.

5. Enter a value for the rising trigger. A rising trigger alarm is generated when the event count per interval exceeds the rising trigger. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and rises again above the rising trigger. Consider the example in Figure 4-8.
6. Enter a value for the falling trigger. A falling trigger alarm is generated when the event count per interval descends below the falling trigger.

Note: The switch will down a port if a rising trigger alarm is not cleared after three consecutive sample windows.

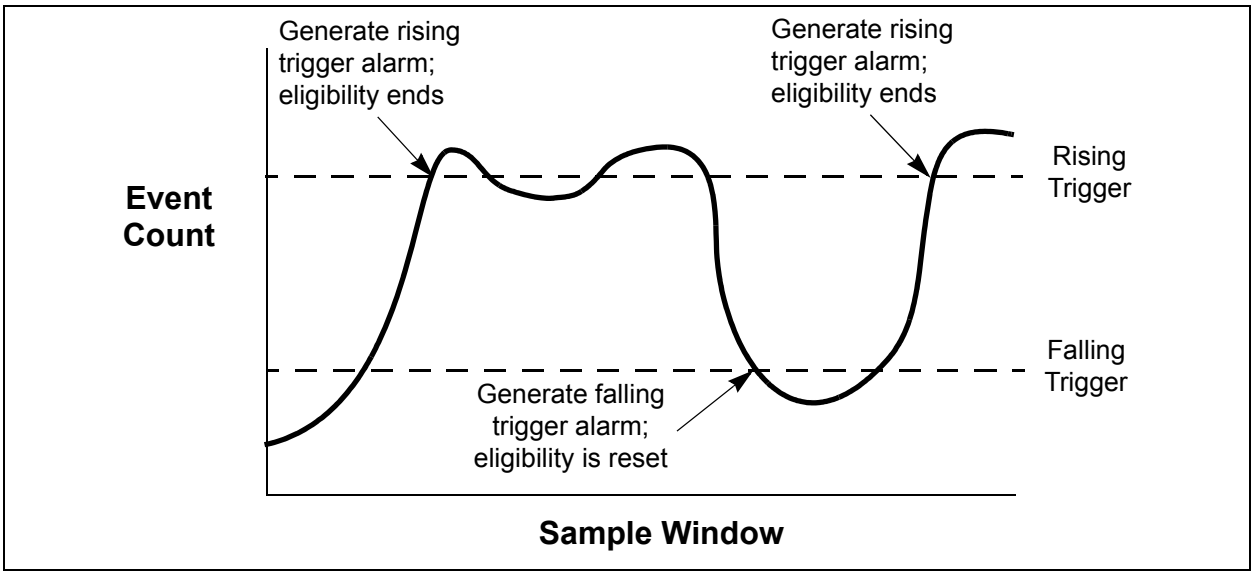


Figure 4-8. Port Threshold Alarm Example

7. Enter a sample window in seconds. The sample window defines the period of time in which to count events.
8. Repeat steps 3 through 7 for each alarm you want to configure or enable.
9. Click the **OK** button to save all changes.

4.4 Paging a Switch

You can use the beacon feature to page a switch. The beacon feature causes all Logged-In LEDs to flash, making it easier to recognize. To page a switch, open the Switch menu in the faceplate display and enable the **Toggle Beacon** selection. To cancel the beacon, reselect **Toggle Beacon**.

4.5 Setting the Date/Time and Enabling NTP Client

The Date/Time and Network Time Protocol (NTP) dialog enables you to manually set the date, time, and time zone on a switch, or to enable the NTP Client to synchronize the date and time on the switch with an NTP server. Enabling the NTP client ensures the consistency of date and time stamps in alarms and log entries. An Ethernet connection to an NTP server is required. When date/time is set or displayed in the firmware, it is always in Universal Time, However, when displayed in the Date/Time dialog, the value is always in local time. The difference between switch and workstation times must not exceed 24 hours, or the switch management application can not connect. To set the date and time on a switch, do the following:

1. Select a switch in the topology display, and open the faceplate display.
2. Open the Switch menu, and select **Set Date/Time...**.
3. Choose one of the following:
   - Enter the year, month, day, time, and time zone in the Switch Date/Time dialog, then click **OK**. The new date and time take effect immediately.
   - Click the **NTP Client Enabled** checkbox to enable the switch to synchronize its time with an NTP server. Enter the IP address of the NTP server. Ethernet connection to NTP server is required. Click the **OK** button to save the settings.

4.6 Resetting a Switch

Resetting a switch reboots the switch using configuration parameters in memory. Depending on the reset type, a switch reset may or may not include a power-on self test or it may or may not disrupt traffic. Table 4-2 describes the types of switch resets.

During a hotreset operation, fabric services will be unavailable for a short period (30-75 seconds depending on switch model). Verify all administrative changes to the fabric (if any) are complete before performing an NDCLA. When upgrading firmware across a fabric using non-disruptive activation, upgrade one switch at a time and allow 75 seconds between switches.

CAUTION! Changes to the fabric may disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications
- Adding, moving or removing devices attached to the switch fabric. This includes powering up or powering down attached devices.
- Adding, moving or removing ISLs or other connections.

Management Interfaces:

After an NDCLA operation is complete, management connections must be re-initiated:

- SANsurfer Switch Manager sessions will re-connect automatically
- Telnet sessions must be restarted manually.

Applicable Code Versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- An NDCLA operation to previous switch code releases is not supported.

Table 4-3. Switch Resets

Type	Description
Hot Reset	Resets a switch without a power-on self test. This reset activates the pending firmware, but does not disrupt switch traffic. If errors are detected on a port during a hot reset, the port is reset automatically.
Reset without POST	Resets a switch without a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.
Hard Reset	Resets a switch with a power-on self test. This reset activates the pending firmware and it is disruptive to switch traffic.

To reset a switch using SANsurfer Switch Manager, do the following:

1. Select the switch to be reset and open the faceplate display.
2. Open the Switch menu and select the **Reset Switch** pull-down menu:
   - Select **Hot Reset** to perform a hot reset.
   - Select **Reset** to perform a standard reset.
   - Select **Hard Reset** to perform a hard reset.

4.7 Configuring a Switch

Switch configuration is divided into three areas: chassis configuration, network configuration, and SNMP configuration. Chassis configuration specifies switch-wide Fibre Channel settings. Network configuration specifies IP settings, remote logging, and the NTP client. SNMP configuration specifies SNMP settings and traps.

You can configure a switch explicitly or you can use the Configuration Wizard. The Configuration Wizard is a series of dialogs that guide you through the chassis, network, and SNMP configuration steps on new or replacement switches.

4.7.1 Using the Configuration Wizard

The Configuration Wizard is a series of dialogs you can use to configure the IP address and other basic parameters on new or replacement switches. The switch will detect the first time use and present the Initial Start dialog, from which the Configuration Wizard can be launched. You can also launch the Configuration Wizard from the Wizards menu in either the topology display or the faceplate display. Open the Wizards menu and select **Configuration Wizard**. Use the Configuration Wizard to configure a new switch in a fabric.

4.7.2
Switch Properties

To open the Switch Properties dialog, open the faceplate display for a switch, open the Switch menu, and select **Switch Properties**. You may also right-click a switch graphic in the topology display or faceplate display, and select **Switch Properties** from the popup menu. After making changes, click the **OK** button to put the new values into effect. Use the Switch Properties dialog to change the following switch configuration parameters:

- Symbolic Name
- Switch Administrative States
- Domain ID and Domain ID Lock
- Fabric Device Management Interface
- Broadcast Support
- In-band Management

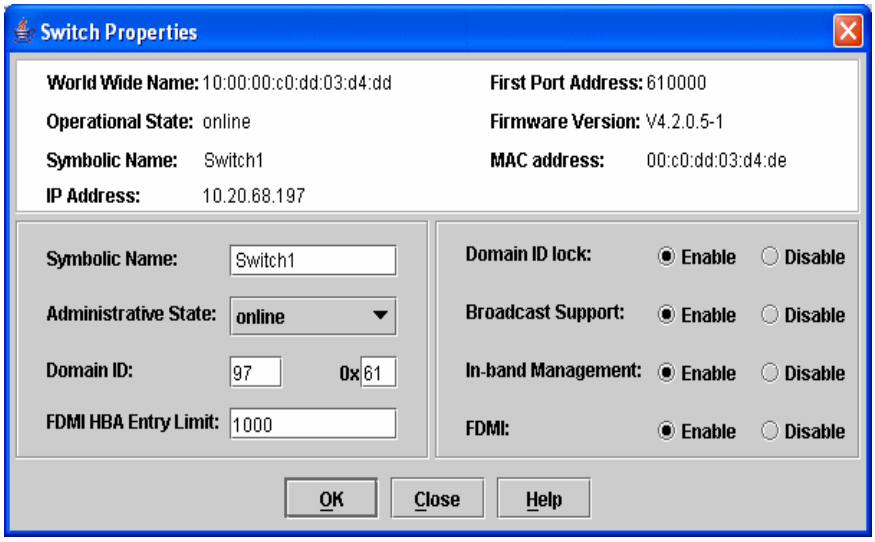


Figure 4-9. Switch Properties Dialog

4.7.2.1
Symbolic Name

The symbolic name is a user-defined name of up to 32 characters that identifies the switch. The symbolic name is used in the topology and faceplate displays, as well as many data windows to more easily identify switches. The illegal characters are the pound sign (#), semi-colon (;), and comma (,).

4.7.2.2
Switch Administrative States

The switch administrative state determines the operational state of the switch. The switch administrative state exists in two forms: the configured administrative state and the current administrative state.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. SANsurfer Switch Manager always makes changes to the configured administrative state. The configured administrative state is displayed in the Switch Properties dialog.
- The current administrative state is the state that is applied to the switch for temporary purposes and is not retained across switch resets. The current administrative state is set using the Set Switch command. Refer to the ”Set Command” on page A-59.

Table 4-4 describes the administrative state values.

Table 4-4. Switch Administrative States

Parameter	Description
Online	The switch is available.
Offline	The switch is unavailable.
Diagnostics	The switch is in diagnostics mode, is unavailable, and tests can then be run on all ports of the switch.

4.7.2.3
Domain ID and Domain ID Lock

The domain ID is a unique Fibre Channel identifier for the switch. The Fibre Channel address consists of the domain ID, port ID, and the Arbitrated Loop Physical Address (ALPA). The maximum number of switches within a fabric is 239 with each switch having a unique domain ID.

Switches come from the factory with the domain IDs unlocked. This means that if there is a domain ID conflict in the fabric, the switch with the highest principal priority, or the principal switch, will reassign any domain ID conflicts and establish the fabric. If you lock the domain ID on a switch and a domain ID conflict occurs, one of the switches will isolate as a separate fabric and the Logged-In LEDs on both switches will flash to show the affected ports. Refer to the ”Set Config Command” on page A-61 for information about the Switch keyword and the Domain ID Lock and Principal Priority parameters.

If you connect a new switch to an existing fabric with its domain ID unlocked, and a domain conflict occurs, the new switch will isolate as a separate fabric. However, you can remedy this by resetting the new switch or taking it offline then back online. The principal switch will reassign the domain ID and the switch will join the fabric.

Note: Domain ID reassignment is not reflected in zoning that is defined by domain ID and port number pair. You must reconfigure zones that are affected by domain ID reassignment.

4.7.2.4
Fabric Device Management Interface

Fabric Device Management Interface (FDMI) provides a means to gather and display device information from the fabric, and allows FDMI capable devices to register certain information with the fabric, if FDMI is enabled. SANsurfer Switch Manager will report any and all FDMI information reported by the entry switch, if FDMI is enabled on the entry switch. To view FDMI data, FDMI must be enabled on the entry switch and on all other switches in the fabric which are to report FDMI data.

FDMI is comprised of the fabric-to-device interface and the application-to-fabric interface. The fabric-to-device interface enables a device’s management information to be registered. The application-to-fabric interface provides the framework by which an application obtains device information from the fabric. Use the **FDMI HBA Entry Limit** field on the Switch Properties dialog to configure the maximum number of HBAs that can be registered with a switch. If the number of HBAs exceeds the maximum number, the FDMI information for those HBAs can not be registered.

Use the **FDMI Enabled** radio button on the Switch Properties dialog to enable or disable FDMI. If FDMI is enabled on an HBA, the HBA forwards information about itself to the switch when the HBA logs into the switch. If FDMI is enabled on a switch, the switch stores the HBA information in its FDMI database. Disabling FDMI on a switch clears the FDMI database. If you disable FDMI on a switch, then re-enable it, you must reset the ports to cause the HBAs to log in again, and thus forward HBA information to the switch.

To view detailed FDMI information for a device, open the topology display, click the **Devices** tab, and click the **Information (i)** button in the Details column of the Devices data window. The Detailed Devices Display dialog displays the specific information for that device. Refer to ”Devices Data Window” on page 3-33 for more information.

4.7.2.5
Broadcast Support

Broadcast is supported on the switch and allows for TCP/IP support. Broadcast is implemented using the proposed standard specified in *Multi-Switch Broadcast for FC-SW-3, T11 Presentation Number T11/02-031v0*. Fabric Shortest Path First (FSPF) is used to set up a fabric spanning tree used in transmission of broadcast frames. Broadcast frames are retransmitted on all ISLs indicated in the spanning tree and all online N_Ports and NL_Ports. Broadcast zoning is supported with Access Control List (ACL) hard zones. When a broadcast frame is received, these hard zones are enforced at the N_Ports and NL_Ports. If the originator of the broadcast is in a hard zone, the frame is retransmitted on all online N_Ports and NL_Ports within the hard zone. If the originator of the broadcast frame is not in a hard zone, the frame is retransmitted on online N_Ports and NL_Ports that are not in a hard zone. The default setting is disabled.

4.7.2.6
In-band Management

In-band management is the ability to manage switches across inter-switch links using SANsurfer Switch Manager, SNMP, management server, or the application programming interface. The switch comes from the factory with in-band management enabled. If you disable in-band management on a particular switch, you can no longer communicate with that switch by means other than a direct Ethernet or serial connection.

4.7.3
Advanced Switch Properties

The Advanced Switch Properties dialog enables you to set the timeout values, Interop Mode, and Legacy Address Format settings. The Advanced Switch Properties dialog is available for only the entry switch, because an in-band switch can not be taken offline. The switch will automatically be taken offline temporarily and will be restored to its original state after the changes are completed. To open the Advanced Switch Properties dialog, open the Switch menu and select **Advanced Switch Properties**. After making changes, click the **OK** button to put the new values into effect.

Use the Advanced Switch Properties dialog to change the following switch configuration parameters:

- Timeout values
- Interop mode for zoning
- Legacy port address format

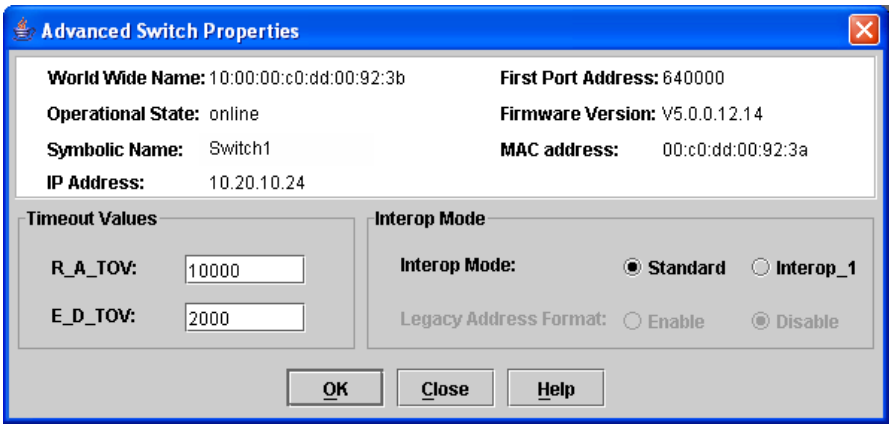


Figure 4-10. Advanced Switch Properties Dialog

4.7.3.1
Interop Mode for Zoning

When a zone set is activated on an FC-SW-2 compliant switch, only the active zone set is propagated to all switches in the fabric. When a zone set is activated on a non-FC-SW-2 compliant switch, the active zone set and all inactive zone sets (the entire zoning database stored in permanent memory) are propagated to all switches in the fabric. Use the Standard option for FC-SW-2 compliant switches to propagate only the active zone set to all switches in the fabric. Use the Interop_1 parameter for non-FC-SW-2 compliant switches to propagate the active zone set and all inactive zone sets to all switches in the fabric.

4.7.3.2
Legacy Port Address Format

Legacy Address Format should be enabled only to permit interoperation with certain older non-FC-SW-2 compliant switches. Enabling this setting under other circumstances will disable zoning that is defined by domain ID and port number. This Legacy Address Format option is available only when the Interop_1 setting is enabled on the Advanced Switch Properties dialog. Contact your authorized maintenance provider for assistance in using this feature. Refer to the QLogic Switch Interoperability Guide on the QLogic Web site for a complete discussion of configuring for operation with non-Qlogic Switches.

Note: The Legacy Address Format setting must be the same on all switches in the fabric, otherwise the inter-switch links will not connect.

4.7.3.3
Timeout Values

The switch timeout values determine the timeout values for all ports on the switch. Table 4-5 describes the switch timeout parameters. The timeout values must be the same for all switches in the fabric.

Note: Mismatched timeout values will disrupt the fabric. These should not be changed unless absolutely necessary. Therefore, the switch must be offline to change these values. Use the Switch Properties dialog to take the switch offline.

Table 4-5. Timeout Values

Parameter	Description
R_A_TOV	Resource Allocation Timeout: Represents the maximum time a frame could be delayed in the Fabric and still be delivered. The default is 10000 milliseconds.
E_D_TOV	Error Detect Timeout: Represents the maximum round trip time that an operation between two N_Ports could require. The default is 2000 milliseconds.

4.7.4
System Services Dialog

The System Services dialog provides a central location for you to enable or disable any of the external user services such as Simple Network Management Protocol (SNMP), Secure Sockets Layer (SSL),Secure SHell (SSH), embedded switch management application, command line interface, Network Time Protocol (NTP), and Common Information Model (CIM). To display the System Services dialog, open the Switch menu and select **Services**.

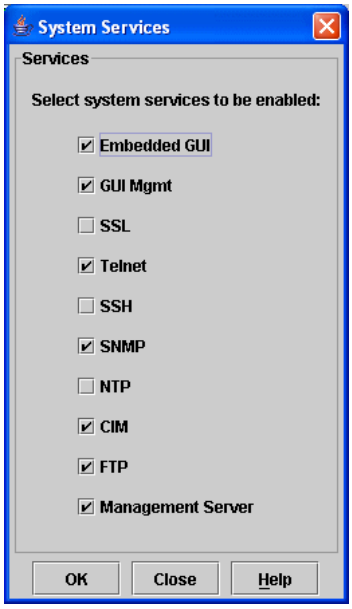


Figure 4-11. System Services Dialog

Use caution when disabling the Embedded GUI, GUI Mgmt, Telnet, SSL, and SSH, as it is possible to disable all access to the switch except through a serial connection.

- **Embedded GUI** - Embedded Graphical User Interface. Allows users to point a browser at the switch and run the embedded switch management application on that switch as an applet.
- **GUI Mgmt** - Allows out-of-band management of the switch from the switch management application (GUI). If disabled, the switch can not be specified as the entry switch for a fabric in the GUI, but can still be managed through an in-band connection.

- **SSL** - Secure Sockets Layer. Provides secure encrypted communications between the switch management application (GUI) and the switch. SSL must be enabled for configuration of security and radius servers with the switch management application (GUI). SSL certificates are generated on the switch with the switch date/time and validated with the workstation's date/time. If the Switch and workstation date/time are not in sync, invalid certificates will be generated and prevent an SSL connection from being established between the switch and switch management application (GUI). To disable SSL when using a user authentication RADIUS server, the RADIUS authentication order must first be set to **Local**.
- **Telnet** - Command line interface. Allows users to manage the switch through a Telnet command line interface session. Disabling Telnet access to the switch is not recommended.
- **SSH** - Secure SHell. Provides secure encrypted Telnet command line interface sessions with the switch. Note that you will have to have an SSH client running on your workstation in order to manage your switch with Telnet command line interface when SSH is enabled.
- **SNMP** - Simple Network Management Protocol. Allows management of the switch through third-party applications that use SNMP.
- **NTP** - Network Time Protocol. Allows the switch to obtain its time and date settings from an NTP server. Configuring all of your switches and your workstations to utilize NTP will keep their date/time settings in sync and will prevent difficulties with SSL certificates and event logs.
- **CIM** - Common Information Model. Allows management of the switch through third-party applications that use CIM.
- **FTP** - File Transfer Protocol. Allows file transfers to the switch via FTP. FTP is required for out-of-band firmware uploads which will complete faster than in-band Firmware uploads.
- **Management Server** - Allows management of the switch through third-party applications that use GS-3 Management Server.

4.7.5 Security Consistency Checklist Dialog

The Security Consistency Checklist dialog enables you to compare security-related features on switches in order to check for inconsistencies. Any changes must be made through the appropriate dialog, such as Network Properties dialog, Switch Properties dialog, or SNMP Properties dialog. To open the Security Consistency Checklist dialog, open the faceplate display, open the Switch menu and select **Security Consistency Checklist**.

4.7.6

Network Properties

Use the Network Properties dialog shown in Figure 4-12 to change IP configuration parameters and enable remote logging. After making changes, click the **OK** button to put the new values into effect. To open the Network Properties dialog, select a switch in the topology display or open the faceplate display, open the Switch menu and select **Network Properties**.

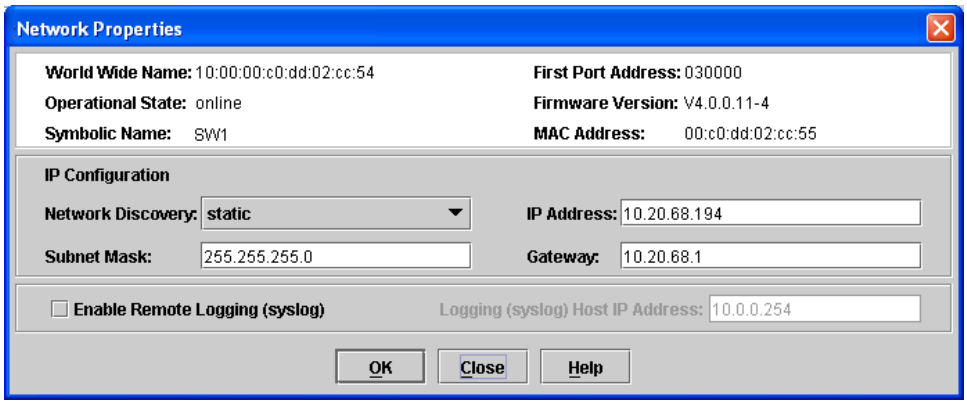


Figure 4-12. Network Properties Dialog

4.7.6.1

IP Configuration

The IP configuration identifies the switch on the Ethernet network and determines which network discovery method to use. Table 4-6 describes the IP configuration parameters.

Table 4-6. IP Configuration Parameters

Parameter	Description
Network Discovery	Choose one of the following methods by which to assign the IP address: ■ Static - Uses the IP configuration parameters entered in the Switch Properties dialog. ■ BootP - Acquires the IP configuration from a BootP server. ■ RARP (Reverse Address Resolution Protocol) - Acquires the IP address from an RARP server. An RARP request is broadcast with up to three retries, each at 5 second intervals. If no IP address is obtained, the switch reverts to the previously configured IP address. ■ DHCP (Dynamic Host Configuration Protocol) - Acquires the IP configuration from a DHCP server. If no satisfactory lease is obtained, the DHCP client attempts to use the previously configured lease. If the previous lease cannot be used, no IP address will be assigned to this switch in order to avoid an IP address conflict. The DHCP server must then be made available. If a BootP, RARP, or DHCP server is not available, the switch will attempt to use a previously assigned valid lease. If no lease was ever assigned, the switch will attempt to use the previously assigned static IP address.
IP Address	Internet Protocol (IP) address for the Ethernet port. The default value is 10.0.0.1.
Subnet mask	Subnet mask address for the Ethernet port. The default value is 255.0.0.0.
Gateway	IP gateway address. The default value is 10.0.0.254.

4.7.6.2
Remote Logging

The Remote Logging (syslog) feature enables saving of the log information to a remote host that supports the syslog protocol. When enabled, the log entries are sent to the syslog host at the IP address that you specify in the Logging Host IP Address field. Log entries are saved in the internal switch log whether this feature is enabled or not.

To save log information to a remote host, you must edit the syslog.conf file (located on the remote host) and then restart the syslog daemon. Consult your operating system documentation for information on how to configure Remote Logging. The syslog.conf file on the remote host must contain an entry that specifies the name of the log file in which to save error messages. Add the following line to the syslog.conf file. A <tab> separates the selector field (local0.info) and action field which contains the log file path name (/var/adm/messages/messages.name).

```
local0.info <tab> /var/adm/messages.name
```

4.7.6.3
NTP Client

The NTP Client feature allows switches to synchronize their date and time with a centralized server. NTP client ensures the consistency of date and time stamps in alarms and log entries. An Ethernet connection to NTP server is required. Refer to ”Setting the Date/Time and Enabling NTP Client” on page 4-16 for more information.

4.7.7
SNMP Properties

Use the SNMP Properties dialog shown in Figure 4-13 to change SNMP configuration parameters. After making changes, click the **OK** button to put the new values into effect. To open the SNMP Properties dialog, select a switch in the topology display or open the faceplate display, open the Switch menu and select **SNMP Properties**.

Note: Since Read Community, Trap Community, and Write Community settings are like passwords and are write-only fields, the current settings are displayed as asterisks.

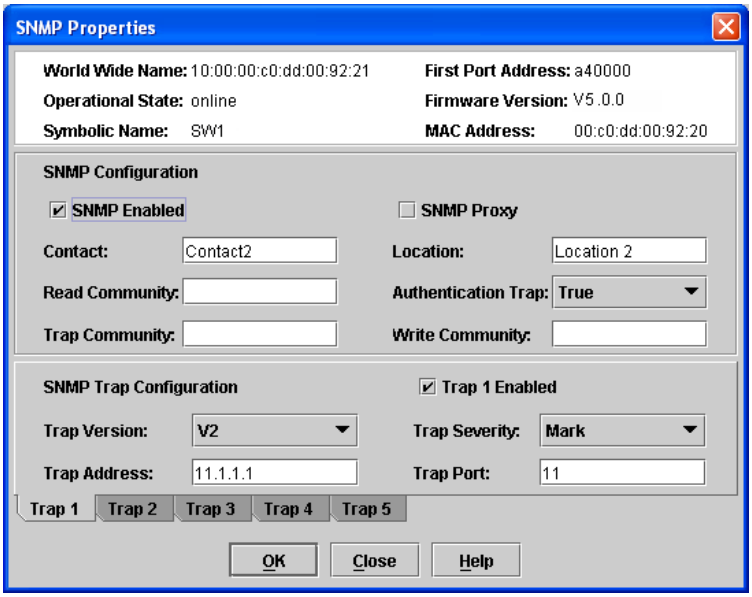


Figure 4-13. SNMP Properties Dialog

4.7.7.1

SNMP Configuration

The SNMP configuration defines how authentication traps are managed.Table 4-7 describes the SNMP configuration parameters. The illegal characters for the user-defined fields are the pound sign (#), semi-colon (;), and comma (,).

Table 4-7. SNMP Configuration Parameters

Parameter	Description
SNMP Enabled	Enables or disables SNMP communication with other switches in the fabric.
Contact	Specifies the name (up to 64 characters) of the person who is to be contacted to respond to trap events. The default is “undefined”.
Read Community	Read community password (up to 32 characters) that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
Trap Community	Trap community password (up to 32 characters) that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “public”.
SNMP Proxy	If enabled, you can use SNMP to monitor and configure any switch in the fabric.
Location	Specifies the name (up to 64 characters) for the switch location. The default is “undefined”.
Authentication Trap	Enables or disables the reporting of SNMP authentication failures. If enabled, a notification trap is sent when incorrect community string values are used. The default value is "False".
Write Community	Write community password (up to 32 characters) that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The default is “private”.

4.7.7.2

SNMP Trap Configuration

The SNMP trap configuration defines how traps are set. Choose from the tabs **Trap1** – **Trap 5** to configure each trap. Table 4-8 describes the SNMP configuration parameters.

Table 4-8. SNMP Trap Configuration Parameters

Parameter	Description
Trap Version	Specifies the SNMP version (1 or 2) with which to format traps.
Trap 1 Enabled	Enables or disables the trap. If disabled, traps are not configurable.
Trap Address[1]	Specifies the IP address to which SNMP traps are sent. A maximum of 5 trap addresses are supported. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0.
Trap Port[1]	The port number on which the trap is sent. The default is 162.
Trap Severity	Specifies a severity level to assign to the trap. Open the pull-down menu and choose a level. The **Trap 1 Enabled** check box on the SNMP Properties dialog must be enabled to access this pull-down menu. Trap severity levels include Unknown, Emergency, Alert, Critical, Error, Warning, Notify, Info, Debug, and Mark

[1]Trap address (other than 0.0.0.0) and trap port combinations must be unique. For example, if trap 1 and trap 2 have the same address, then they must have different port values. Similarly, if trap 1 and 2 have the same port value, they must have different addresses.

4.8 Managing Switch Stacks

SANsurfer Switch Manager recognizes switches as a stack if they are connected by their high speed stacking ports. The switch management application will auto-detect switches connected by their 10-Gbps ports and display these stacked switches as a single stack entity in the topology and faceplate displays.

The graphic window (upper right pane of the faceplate display) displays one faceplate image for each switch in the stack.

In the fabric tree (left pane of the faceplate display), the switches in each stack are nested under the stack icon, which is nested under the fabric icon. Expanding the fabric and stack icons in the fabric tree displays all switches in a stack. The lock image on the fabric icon indicates that the application is communicating with the fabric through a secure (Secure Sockets Layer) connection.

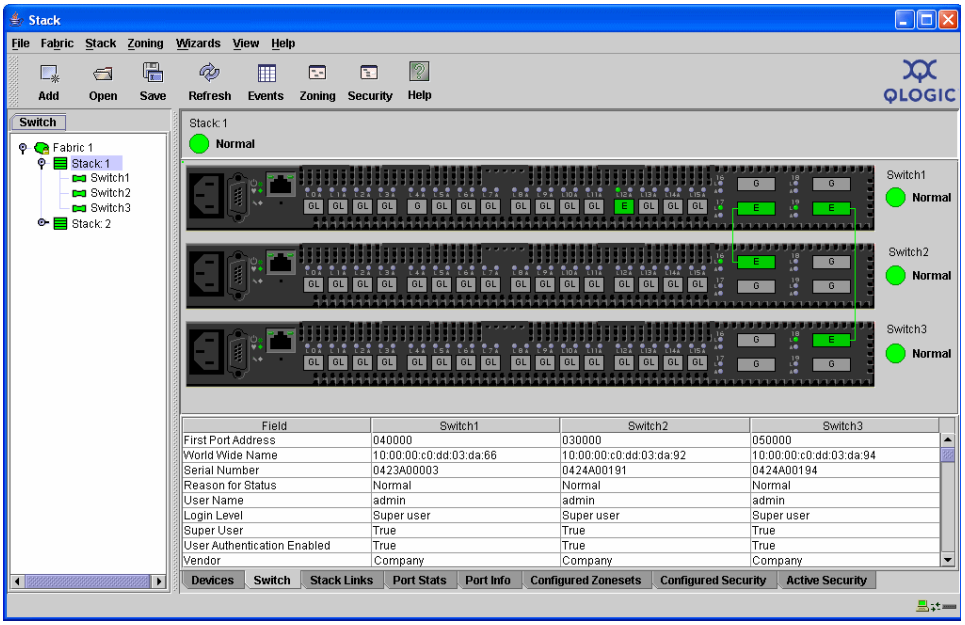


Figure 4-14. Switch Stacks

The stack dialogs are essentially the same as their corresponding switch dialogs, except for the Select Switch for Initial Configuration pull-down menu is added to each dialog. The stack dialogs display the information for the switch selected in the Select Switch for Initial Configuration pull-down menu. Choose another switch in the pull-down menu to display information for that switch. The switch configuration displayed is the configuration that will be applied to all other switches in the stack after you click the OK button. The following operations are available to configure the stack as a single entity:

- Date/time and Network Time Protocol (NTP) settings. Refer to ”Setting the Date/Time and Enabling NTP Client” on page 4-16 for more information.
- Firmware load and activation. Refer to ”Installing Firmware” on page 4-42 for more information.
- Switch reset. Refer to ”Resetting a Switch” on page 4-16 for more information.
- Edit zoning configuration. Refer to ”Configuring the Zoning Database” on page 3-46 for more information.
- Editing user accounts. Refer to ”Managing User Accounts” on page 4-1 for more information.
- SNMP configuration. Refer to ”SNMP Configuration” on page 4-31 for more information.
- Syslog configuration. Refer to ”Syslog” on page 4-35 for more information.

Additional stack operations include:

- Refresh the stack to update the faceplate display with current information for all switches in the stack
- Select all ports on all switches in the stack
- Remove a switch from a stack. Choose this option after a switch no longer has a 10-Gbps link. The switch icon is moved from the stack icon and becomes a single switch icon in the topology display.

4.8.1 Syslog

The Syslog dialog enables you to save the log information for the stack to a remote host that supports the syslog protocol. Use the Syslog dialog to enable remote logging for the stack. Refer to ”Remote Logging” on page 4-29 for more information.

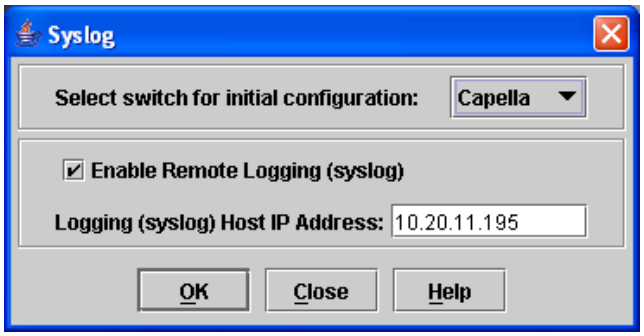


Figure 4-15. Syslog Dialog

4.8.2 Select Source Dialog

The Select Source dialog enables you to select the initial zoning configuration to be loaded into the Edit Zoning dialog when making zoning changes to all switches in a stack. The Select Source dialog is only displayed if the zoning configuration on all switches in the stack is not identical. To display the Select Source dialog, select a switch stack icon in the fabric tree (left-pane), open the Zoning menu and select **Edit Zoning**. Select a switch in the Source Switch list and click the **OK** button to open the Edit Zoning dialog with the zoning configuration of the selected (source) switch displayed. The zoning changes made to the source switch in the Edit Zoning dialog are applied to all switches in the stack.

4.9 Archiving a Switch

You can create an .XML archive file containing the configuration parameters. Basically any data received by SANsurfer Switch Manager is archived. However, passwords are not archived with the user account information. Archived parameters include the following:

- Switch properties and statistics
- IP configuration
- SNMP configuration
- Port properties and statistics
- Alarm configuration
- Zoning configuration
- Configured security
- RADIUS Server information

This archive file can be used to restore the configuration on the same switch or on a replacement switch. You can also use the archive file as a template for configuring new switches to add to a fabric. User account information is not archived. The archive can be used later to restore the switch. Refer to ”Restoring a Switch” on page 4-37 for more information.

To archive a switch, do the following:

1. Open the Switch menu in the faceplate display and select **Archive**.
2. In the Save dialog, enter a file name.
3. Click the **Save** button.

4.10 Restoring a Switch

Restoring a switch loads the archived switch configuration parameters to the switch. The switch configuration must be archived before it can be restored. The switch archive must be compatible with the switch to be restored; that is, you can restore a SANbox 5602 switch only with an archive from a SANbox 5602 switch. Refer to ”Archiving a Switch” on page 4-36 for more information.

CAUTION! The switch being restored should be physically disconnected from the fabric. Restoring a switch in a fabric can severely disrupt the fabric. After the restore process is complete, the switch can be reconnected to the fabric.

To restore a switch, do the following:

1. Log in to the fabric through the switch you want to restore. You cannot restore a switch over an ISL.
2. Open the Switch menu in the faceplate display and select **Restore** to display the Restore dialog shown in Figure 4-16. The Restore dialog offers a **Full Restore** and a **Selective Restore** tab.

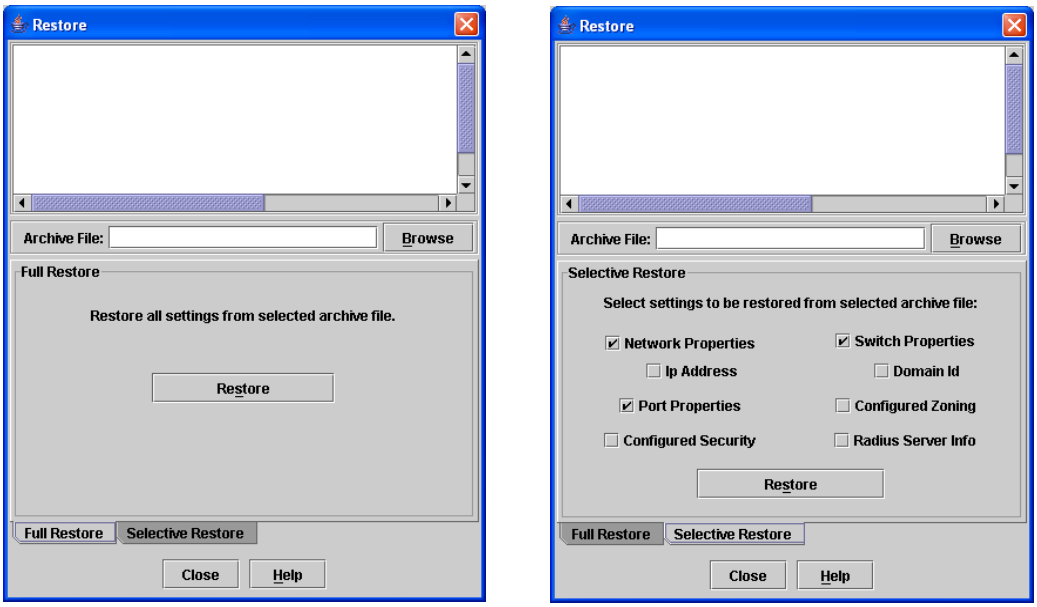


Figure 4-16. Restore Dialogs – Full and Selective

3. Enter the archive file name or browse for the file. This archive file must be one that was produced by the SANsurfer Switch Manager Archive function. Configuration backup files created with the Config Backup command are not compatible with the SANsurfer Switch Manager Restore function.
4. To restore all configuration settings, click the **Full Restore** tab, then click the **Restore** button. To restore selected configuration settings, click the **Selective Restore** tab and check one or more of the following boxes, then click the **Restore** button:
   - **Network Properties**: Restores all settings presented in the Network properties dialog except the IP address. Refer to ”Network Properties” on page 4-27.
   - **IP Address**: Restores switch IP address in addition to the other network properties.
   - **Switch Properties:** Restores all settings presented in the Switch properties dialog except the domain ID. Refer to ”Switch Properties” on page 4-19.
   - **Domain ID:** Restores switch domain ID in addition to the other switch properties.
   - **Port Properties**: Restores all settings presented in the Port properties dialog. Refer to ”Configuring Ports” on page 5-10.
   - **Configured Zoning**: Restores all configured zone sets, zones, and aliases in the switch’s zoning database excluding the active zone set.
   - **Configured Security**: Restores all security sets in the switch database.
   - **Radius Server**: Restores all RADIUS Server information defined in the switch database.
5. If you select the Configured Zoning or Full Restore option and the file contains zone sets, a dialog prompts you to activate one of those zone sets. Click the **Yes** button, and select a zone set from the drop-down menu in the Select Zone Set to be Activated dialog.
6. Click the **OK** button and view the results in the top pane of the Restore dialog.

4.11 Restoring the Factory Default Configuration

You can restore the switch and port configuration settings to the factory default values. To restore the factory configuration on a switch, open the Switch menu and select **Restore Factory Defaults**. Table 4-9 lists the factory default switch configuration settings.

Restoring the switch to the factory default configuration does not restore the account name and password settings. The most current port license will remain in effect. To restore user accounts, you must select the **Reset Password File** option in the maintenance menu. Refer to “Recovering a Switch” in the Installation Guide for your switch for information about maintenance mode and the maintenance menu.

Table 4-9. Factory Default Configuration Settings

Setting	Value
Symbolic Name	SANbox
Administrative State	Online
Domain ID	1
Domain ID Lock	False
In-band Management	True
Broadcast Support	Enable
Resource Allocation Timeout (R_A_TOV)	10000 milliseconds
Interop Mode	True
I/O Stream Guard	Disabled
Device Scan Enabled	True
Error Detect Timeout (E_D_TOV)	2000 milliseconds
SNMP Enabled	True
SNMP Proxy	True
IP Address	10.0.0.1
FDMI Enabled	True
FDMI HBA Entry Level	1000
Subnet Mask Address	255.0.0.0
Gateway Address	10.0.0.254

Table 4-9. Factory Default Configuration Settings (Continued)

Setting	Value
Network Discovery	Static
Remote Logging	False
Remote Logging Host Ip Address	10.0.0.254
NTP Client Enabled	False
NTP Server IP Address	10.0.0.254
Contact	Undefined
Location	Undefined
Trap Enabled	False
Trap Port	162
Trap Address	Trap 1: 10.0.0.254; Traps 2-5: 0.0.0.0
Trap Community	Public
Read Community	Public
Write Community	Private
Port State	Online
Port Speed	Auto-detect
Port Type	1-Gbps/2-Gbps/4-Gbps = GL, 10-Gbps = G

4.12 Downloading a Support File

The Download Support File menu option assembles all log files and switch memory data into a core dump file (dump_support.tgz). This file can be sent to technical support personnel for troubleshooting switch problems. The menu option is not accessible (displayed) for switches that don't support the download support file function.

To create a support file, do the following:

1. On the faceplate display, open the Switch menu, and select **Download Support File**.
2. In the Download Support File dialog, click the **Browse** button to define a location for the support file or type the path in the text field.
3. Click the **Start** button to begin the process of creating and downloading the support file to your workstation. Observe the status in the Status area.
4. After the support file is saved to your workstation, click the **Close** button to close the Download Support File dialog.

4.13 Upgrading the Switch Using License Keys

A (port) license key is a password that you can purchase from your switch distributor or authorized reseller to upgrade your switch. The port license keys vary according to the features you purchase. A port license key enables you to:

- Upgrade the switch to a 12-, 16-, or 20-port switch. The switch can come from the factory as an 8-, 12-, 16-, or 20-port switch enabling ports 0-7, 0-11, 0-15, or 0-20 respectively.
- Upgrade the switch to enable 4-Gbps port speed support.

Note: Upgrading a switch using a port key license through an in-band switch is not recommended because traffic may be disrupted. However, SANsurfer Switch Manager does not prevent the user from doing so.

To upgrade a switch using a port license key, do the following:

1. Isolate the switch from the fabric.
2. Add a fabric with the IP address of the switch you want to upgrade.
3. Open the faceplate display for the switch you want to upgrade.

4. Open the Switch Menu and select **Features** to open the Feature Licenses dialog shown in Figure 4-17.

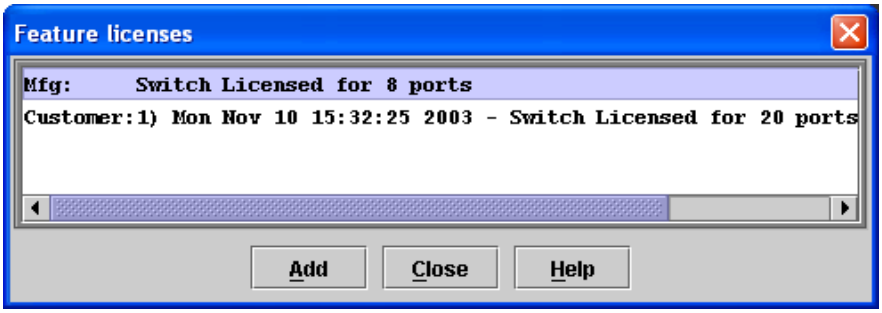


Figure 4-17. Features License Key Dialog

5. In the Feature Licenses dialog, click the **Add** button to open the Add License Key dialog shown in Figure 4-18.

Figure 4-18. Add License Key Dialog

6. In the Add License Key dialog, enter the port license key in the Key field.
7. Click the **Description** button to display and view the upgrade description.
8. Click the **Add Key** button to upgrade the switch. Allow a minute or two for the upgrade to complete. The switch will need to be reset after the upgrade.

4.14 Installing Firmware

Installing firmware involves loading, unpacking, and activating the firmware image on the switch. SANsurfer Switch Manager does this in one operation. To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

The pending firmware version will differ from the active version during the brief period while the switch is resetting to activate the firmware. Firmware management tools enable you to install and activate new firmware.

During a hotreset operation, fabric services will be unavailable for a short period (30-75 seconds depending on switch model). To ensure that an NDCLA operation is successful, verify that all administrative changes to the fabric (if any) are complete. When you need to do NDCLA/hotreset to multiple switches, only perform the NDCLA/hotreset on one switch at a time, and allow a 75 second wait before performing the NDCLA/hotreset operation on the next switch.

CAUTION! Changes to the fabric may disrupt the NDCLA process.

Common administrative operations that change the fabric include:

- Zoning modifications
- Adding, moving or removing devices attached to the switch fabric. This includes powering up or powering down attached devices.
- Adding, moving or removing ISLs or other connections.

Management Interfaces:

After an NDCLA operation is complete, management connections must be re-initiated:

- SANsurfer Switch Manager sessions will re-connect automatically
- Telnet sessions must be restarted manually.

Applicable Code Versions:

- Future switch code releases will be upgraded non-disruptively unless specifically indicated in its associated release notes
- An NDCLA operation to previous switch code releases is not supported.

To install firmware, do the following:

1. In the faceplate display, open the Switch menu and select **Load Firmware**.
2. In the Firmware Upload dialog, click the **Browse** button to browse and select the firmware file to be uploaded.
3. Click the **Start** button to begin the firmware load process. You will be shown a message warning you that the switch will be reset in order to activate the firmware.
4. SANsurfer Switch Manager prompts you to activate the new firmware using a hot (non-disruptive) reset, if possible. Click the **OK** button to reset the switch and activate the new firmware.

4.14.1
Displaying Hardware Status

To display a summary of the hardware status information in a popup text box, rest the cursor over the chassis LED cluster in the faceplate display.

- Input Power LED - indicates the voltage status of the switch.
- Heartbeat LED - indicates the status of the internal switch processor and the results of the POST.
- System Fault LED - indicates an over temperature condition or a Power On Self Test error.

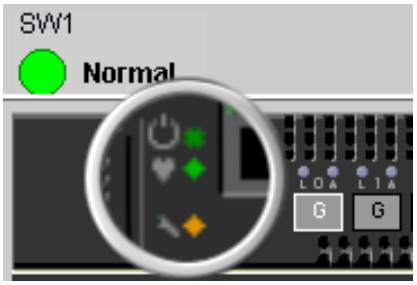


Figure 4-19. Hardware Status LEDs

Section 5

Managing Ports

This section describes the following tasks that manage ports and devices:

- Displaying Port Information
- Configuring Ports
- Using the Extended Credits Wizard
- Resetting a Port
- Testing Ports
- Graphing Port Performance

5.1 Displaying Port Information

Port information is available primarily in the faceplate display shown in Figure 5-1. The faceplate display data windows provide information and statistics for switches and ports. Use the topology display to view status information on fabrics, switches, and links between switches.

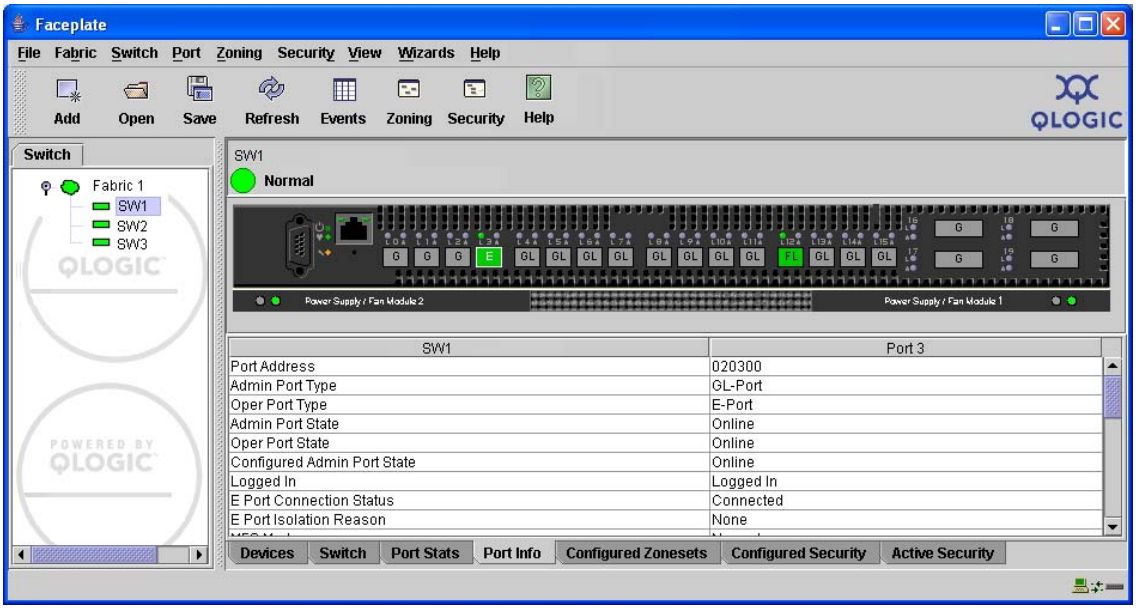


Figure 5-1. Faceplate Display – Port Information

5.1.1
Monitoring Port Status

The faceplate display provides the following port related information:

- Port type
- Port operational state
- Port speed
- Port media

To display port number and status information for a port, position the cursor over a port on the faceplate display. The status information changes depending on the View menu option selected.

5.1.1.1
Displaying Port Types

To display port type status, from the faceplate display, open the View menu, and select **View Port Types**. Table 5-1 lists the possible port types and their meanings.

Table 5-1. Port Types

State	Description
F_Port	Fabric port - Supports a single public device (N_Port).
FL_Port	Fabric loop port - Self discovers a single device (N_Port) or a loop of up to 126 public devices (NL_Port). 1-Gbps/2-Gbps only.
G_Port	Generic port - Self discovers as an F_Port or an E_Port.
GL_Port	Generic loop port - Self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default port type. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port. 1-Gbps/2-Gbps only.
E_Port	Expansion port - The mode that a G_Port or GL_Port is in when attached by an ISL (inter-switch link) to another fibre channel switch.
Donor	Donor port - Allows buffer credits to be used by another port. 1-Gbps/2-Gbps only.

5.1.1.2

Displaying Port Operational States

To display the operational state on each port in the faceplate display, open the View menu and select **View Port States**. Table 5-2 lists the possible operational states and their meanings. The port operational state refers to actual port state and not the administrative state you may have assigned.

Table 5-2. Port Operational States

State	Description
On	Online – port is active and ready to send data.
Ia	Inactive – port operational state is offline, but administrative state is online.
Iso	Isolated – E_Port has lost its connection. Refer to ”Port Information Data Window” on page 5-8 for information about why the E_Port has isolated.
Off	Offline – port is active, can receive signal, but cannot accept a device login.
Dia	Diagnostics – port is in diagnostics mode in preparation for testing
Dn	Down – the port is disabled, power is removed from the lasers, and can’t be logged in.

5.1.1.3

Displaying Port Speeds

To display the speed of each port in the faceplate display, open the View menu and select **View Port Speeds**. Table 5-3 lists the possible port speeds.

Table 5-3. Port Speeds

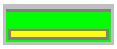
State	Description
Au	Auto-detect
1G	1-Gbps transmission speed
2G	2-Gbps transmission speed
4G	4-Gbps transmission speed (available only with a port license key)
10G	10-Gbps transmission speed

5.1.1.4

Displaying Transceiver Media Status

To display transceiver media status, open the View menu and select **View Port Media**. Table 5-4 lists the port media states and their meanings.

Table 5-4. Port Transceiver Media View

Media Icon	Description
	Optical SFP, Online (Green)
	Optical SFP, Offline (Gray)
	Copper SFP, Online (Green)
	Copper SFP, Offline (Gray)
	XPAK Interface, Online (Green)
	XPAK Interface, Offline (Gray)
None	Empty port, no transceiver installed

5.1.2
Port Statistics Data Window

The Port Statistics data window displays statistics about port performance. To open the Port Statistics window, select one or more ports in the faceplate display and click the **Port Stats** tab below the data window. Table 5-5 describes the Port Statistics data window entries.

The Statistics pull-down menu is available on the Port Statistics data window, and provides different ways to view detailed port information. Click the down arrow to open the pull-down menu. Open the pull-down menu and select **Absolute** to view the total count of statistics since the last switch or port reset. Select **Rate** to view the number of statistics counted per second over the polling period. Select **Baseline** to view the total count of statistics since the last time the baseline was set. When viewing baseline statistics, click the **Clear Baseline** button to set the current baseline. The baseline will also be set when the switch status changes from unreachable to reachable.

Table 5-5. Port Statistics Data Window Entries

Entry	Description
Start Time	The beginning of the period over which the statistics apply. The start time for the Absolute view is not applicable. The start time for the Rate view is the beginning of polling interval. The start time for the Baseline view is the last time the baseline was set.
End Time	The last time the statistics were updated on the display.
Total Time	Total time period from start time to end time.
Al Init	Number of times the port entered the initialization state.
AL Init Error	Number of times the port entered initialization and the initialization failed. Increments count when port has a sync loss.
Bad Frames	Number of frames that were truncated due to a loss of sync or the frame didn't end with an EOF.
Class 2 Frames In	Number of class 2 frames received by this port.
Class 2 Frames Out	Number of class 2 frames transmitted by this port.
Class 2 Words In	Number of class 2 words received by this port.
Class 2 Words Out	Number of class 2 words transmitted by this port.
Class 3 Frames In	Number of class 3 frames received by this port.
Class 3 Frames Out	Number of class 3 frames transmitted by this port.

Table 5-5. Port Statistics Data Window Entries (Continued)

Entry	Description
Class 3 Toss	Number of class 3 frames that were discarded by this port. A frame can be discarded because of detection of a missing frame (based on SEQ_CNT), detection of an E_D_TOV timeout, receiving a reject frame, or receiving a frame on an offline port.
Class 3 Words In	Number of class 3 words received by this port.
Class 3 Words Out	Number of class 3 words transmitted by this port.
Decode Errors	Number of invalid transmission words detected during decoding. Decoding is from the 10-bit characters and special K characters.
Ep Connects	Number of E_Port logins.
FBusy	Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_port that is preventing delivery of this frame.
Flow Errors	Number of times a frame is received and all the switch ports receive buffers are full. The normal Fabric Login exchange of flow control credit should prevent this from occurring. The frame will be discarded.
FReject	Number of frames, from devices, that have been rejected. Frames can be rejected for any of a large number of reasons.
Invalid CRC	Number of invalid Cyclic Redundancy Check (CRC) frames detected.
Invalid Destination Address	Number of address identifier (S_ID, D_ID) errors. AL_PA equals non-zero AL_PA found on F_Port.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or by loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
LIP (AL_PD,AL_PS)	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP(f7,AL_PS)	This LIP is used to reinitialize the loop. An L_port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.

Table 5-5. Port Statistics Data Window Entries (Continued)

Entry	Description
LIP(f7,f7)	A loop initialization primitive frame used to acquire an AL_PA.
LIP(f8,AL_PS)	This LIP denotes a loop failure detected by the L_port identified by AL_PS.
LIP(f8,f7)	A loop initialization primitive frame used to indicate that a Loop Failure has been detected at its receiver and does not have a valid AL_PA.
Login Count	Number of device logins that have occurred on the switch.
Logout Count	Number of device logouts that have occurred on the switch.
Loop Timeouts	Number of loop timeouts.
Loss Of Sync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
Primitive Sequence Errors	Number of bad primitives received by the port.
Rx Link Resets	Number of link reset primitives received from an attached device.
Rx Offline Sequences	Number of offline sequence primitives received by the port.
Total Errors	Total number of primitive and non-primitive port link errors.
Total Link Resets	Number of link-reset primitives transmitted and received by the port.
Total LIPs Received	Number of loop initialization primitive frames received.
Total LIPs Transmitted	Number of loop initialization primitive frames transmitted.
Tx Offline Sequences	Number of offline primitives transmitted by the port.
Total Rx Frames	Total number of frames received by the port.
Total Rx Words	Total number of words received by the port.
Total Tx Frames	Total number of frames transmitted by the port.
Total Tx Words	Total number of words transmitted by the port.
Tx Link Resets	Number of link reset primitives sent from this port to an attached port.
Total Offline Sequences	Total number of offline sequences transmitted and received by the port.

5.1.3
Port Information Data Window

The Port Information data window displays detail information for the selected port. To open the Port Information data window, click the **Port Info** tab below the data window in the faceplate display.

Table 5-6. Port Information Data Window Entries

Entry	Description
Port Address	Port Fibre Channel address.
Administrative Port Type	The administrative port type (G, GL, F, FL, or Donor). This value is persistent; it will be maintained during a switch reset. During port auto-configuration, it will be used to determine which operational port states are allowed.
Operational Port Type	The port type that is currently active. This will be set during port auto-configuration based on the administrative port type.
Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) which has been set by the user. This state may be different from the configured administrative state if the user has not saved it in the switch configuration. This state is used at the time it is set to try to set the port operational state. This value is not persistent and will be lost on a switch reset.
Operational Port State	The port state that is currently active. This value may be different from the administrative port state, for example due to an error condition.
Configured Administrative Port State	The port state (Online, Offline, Diagnostics, or Down) which is saved in the switch configuration, either by the user or at the factory. This value is persistent; it will be maintained during a switch reset, and will be used after a reset to set the port operational state.
Logged In	Indicates whether logged in or not.
E Port Connection Status	E_Port connection status. Status can be None, Connecting, Connected or Isolated.
E Port Isolation Reason	Why E_Port is isolated.
MFS Mode	Multiple Frame Sequence bundling status.

Table 5-6. Port Information Data Window Entries (Continued)

Entry	Description
I/O Stream Guard	RSCN message suppression status. Status can be enabled, disabled, or automatically determined by the switch.
Administrative Port Speed	The speed requested by the user.
Operational Port Speed	The speed actually being used by the port.
Max Credits	The maximum number of credits granted to a port that can be used when extending port credits.
Device Scan	Device scan status. Enabled means the switch queries the connected device during login for FC-4 descriptor information.
Symbolic Name	Port symbolic name
Ext Credits Requested	Number of requested credits
Credits to Donate	The number of credits available to be donated by the selected port.
Donor Group	The donor group of the selected port.
Valid Donor Groups	The number of separate groups within which extended credits may be donated and assigned.
Media	The transceiver type. The 10-Gbps ports always display "unknown", if attached.
Media Speed	The maximum transceiver speed
Media Type	The transceiver fibre type, such as single mode, multi-mode, copper.
Media Transmitter	The transceiver transmitter type, such as longwave, shortwave, electrical.
Media Distance	The maximum transceiver transmission distance
Media Vendor	The company that manufactured the SFP
Media Vendor ID	The IEEE registered company ID
Media Part Number	The part number assigned to the SFP
Media Revision	Transceiver hardware version

5.2 Configuring Ports

The port settings or characteristics for 1-Gbps/2-Gbps/4-Gbps and 10-Gbps ports are configured using the Port Properties dialogs shown in Figure 5-2. To open the corresponding type of Port Properties dialog, select one or more ports, open the Port menu and select **Port Properties** or **Port Properties 10G**.

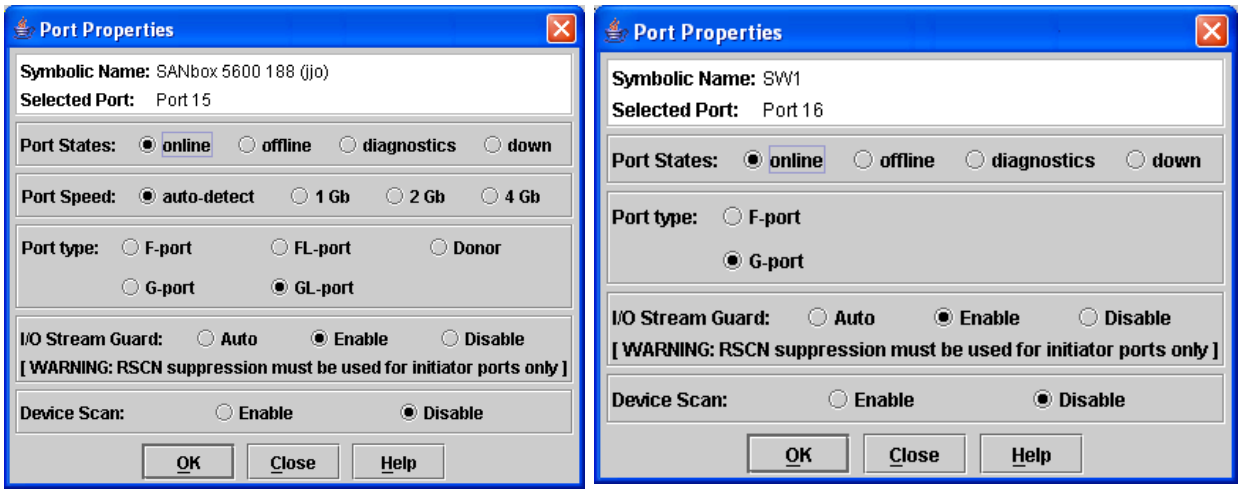

Port Properties
Symbolic Name: SANbox 5600 188 (jjo)
Selected Port: Port 15
Port States: online offline diagnostics down
Port Speed: auto-detect 1 Gb 2 Gb 4 Gb
Port type: F-port FL-port Donor
G-port GL-port
I/O Stream Guard: Auto Enable Disable
[WARNING: RSCN suppression must be used for initiator ports only]
Device Scan: Enable Disable
OK Close Help
Port Properties
Symbolic Name: SW1
Selected Port: Port 16
Port States: online offline diagnostics down
Port type: F-port
G-port
I/O Stream Guard: Auto Enable Disable
[WARNING: RSCN suppression must be used for initiator ports only]
Device Scan: Enable Disable
OK Close Help

Figure 5-2. Port Properties Dialog

The 1-Gbps/2-Gbps/4-Gbps and 10-Gbps Port Properties dialogs displays the switch name and the selected ports. Use the Port Properties dialogs to change the following parameters:

- Port state
- Port speed (1-Gbps/2-Gbps/4-Gbps only)
- Port type
- I/O Stream Guard (RSCN Suppression)
- Device scan

5.2.1
Changing Port Administrative States

The port administrative state determines the operational state of a port. The port administrative state has two forms: the configured administrative state and the current administrative state.

- The configured administrative state is the state that is saved in the switch configuration and is preserved across switch resets. SANsurfer Switch Manager always makes changes to the configured administrative state.
- The current administrative state is the state that is applied to the port for temporary purposes and is not preserved across switch resets. The current administrative state is set using the Set Port command. Refer to the ”Set Port Command” on page A-79.

Table 5-7 describes the port administrative states. To change port administrative state, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties** or **Port Properties 10G** to open the Port Properties dialog.
3. Click the **Port States** radio button that corresponds to the port state you want.
4. Click the **OK** button to write the new port state to the switch.

Table 5-7. Port Administrative States

State	Description
Online	Activates and prepares port to send data.
Offline	Prevents port from receiving signal and accepting a device login.
Diagnostics	Prepares port for testing and prevents the port from accepting a device login.
Down	Disables the port.

5.2.2
Changing Port Speeds

The 1-Gbps/2-Gbps/4-Gbps ports are capable of transmitting and receiving at 1-Gbps or 2-Gbps. The ports can be configured for either transmission speed or to sense the transmission speed of the device to which it is connected. Table 5-8 describes the port speeds. To change the port speed, do the following:

1. Select one or more 1-Gbps/2-Gbps/4-Gbps ports in the faceplate display.
2. Open the Port menu and select **Port Properties**.
3. Click the Port Speed radio button you want.
4. Click the **OK** button to write the new port speed to the switch.

Table 5-8. Port Speeds

State	Description
Auto-Detect	Matches the transmission speed of the connected device. This is the default.
1 Gb	Sets the transmission speed to 1-Gbps.
2 Gb	Sets the transmission speed to 2-Gbps.
4 Gb	Sets the transmission speed to 4-Gbps. (Available only with a port license key.)

5.2.3
Changing Port Types

The ports can be configured to self-discover the proper type to match the device or switch to which it is connected. Table 5-9 describes the port types.

To change the port type, do the following:

1. Select one or more ports in the faceplate display.
2. Open the Port menu and select **Port Properties 1G/2G** or **Port Properties 10G** to open the Port Properties dialog.
3. Click the **Port Type** radio button for the port type you want.
4. Click the **OK** button to write the new port type to the switch.

Table 5-9. Port Types

State	Description
F_Port	Fabric port - Supports a single public device (N_Port).
FL_Port	Fabric loop port - Self discovers a single device (N_Port) or a loop of up to 126 public devices (NL_Port). 1-Gbps/2-Gbps only.
G_Port	Generic port - Self discovers as an F_Port or an E_Port.
GL_Port	Generic loop port - Self discovers as an F_Port, FL_Port, or an E_Port. GL_Port is the default port type. A single device on a public loop will attempt to configure as an F_Port first, then if that fails, as an FL_Port. 1-Gbps/2-Gbps/4-Gbps only.
Donor	Donor port - Allows buffer credits to be used by another port. 1-Gbps/2-Gbps/4-Gbps only.

5.2.4
I/O Stream Guard

The I/O Stream Guard feature suppresses the Registered State Change Notification (RSCN) messages on a port basis. I/O Stream Guard should be enabled only on ports connected to initiator devices. To configure the I/O Stream Guard option using the Port Properties dialog, open the Port menu, and select **Port Properties**. Click the radio button that corresponds to one of the following:

- Enable: Suppresses the reception of RSCN messages from other ports for which I/O Stream Guard is enabled.
- Disable: Allows free transmission and reception of RSCN messages.
- Auto: Suppresses the reception of RSCN messages when the port is connected to an initiator device with a QLogic HBA. For older QLogic HBAs, such as the QLA2200, Device Scan must be enabled. The default is Auto.

5.2.5
Device Scan

The Device Scan feature queries the connected device during login for FC-4 descriptor information. Disable this parameter only if the scan creates a conflict with the connected device.

5.2.6
Changing Port Symbolic Name

To change the symbolic name of a port from the faceplate display, do the following:

1. Open the faceplate display and select a port.
2. Open the Port menu and select **Port Symbolic Name**.
3. In the Port Symbolic Name dialog, choose one of the following:
   - Enter a new name for the port in the Set Port Symbolic Name field.
   - Check the **Restore Default Port Symbolic** Name check box to restore the default name.
4. Click the **OK** button.

5.3
Using the Extended Credits Wizard

Each port is supported by a data-buffer with a 16-credit capacity; that is, 16 maximum sized frames. For fiber optic cables, this enables full bandwidth service over a distance of 26 kilometers at 1-Gbps (0.6 credits per Km), 13 kilometers at 2-Gbps (1.2 credits per Km), or 6 kilometers at 4-Gbps (2.4 credits per Km). Longer distances can be spanned at full bandwidth by borrowing credits from designated donor ports thus pooling the buffer capacities. This is called credit extension. Each donor port contributes 15 credits to the pool from which the recipient ports can draw. The recipient port also loses one credit in the process. For example, one donor port contributes 15 credits to the pool from which a recipient draws for a total of 30 credits (15+15). This provides approximately 50 Km at 1-Gbps (30÷0.6), 25 Km at 2-Gbps (30÷1.2), or 13 Km at 4-Gbps (30÷2.4).

Only 1-Gbps/2-Gbps/4-Gbps ports can donate or borrow credits. To extend credits, open the Wizards menu and select **Ext Credit Wizard**. The Extended Credit Wizard leads you through the following process to extend credits based on transmission distance requirements:

1. Extended Distance: Explains the concepts and principles of extending port credits. Click the **Next** button.
2. Extended Distance Requirements: Specify speed and distance requirements for each port then click the **Next** button.

3. Designate Donor Ports: Select available ports and click **>>** to move the port into the Selected Donor Port column shown in Figure 5-3. Match the number of ports needed with the number of designated donor ports. Click the **Next** button.

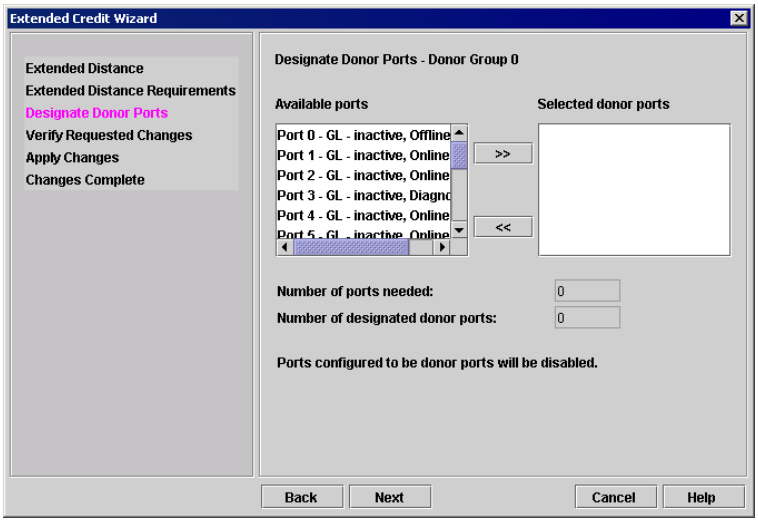


Figure 5-3. Designate Donor Ports

4. Verify Requested Changes: Review the extended distance requests and the selected donor ports. Click the **Finish** button to apply the changes, and redistribute the credits.

Note: As credits are used, the Logged-In LEDs on the corresponding donor ports illuminate continuously. In addition, donor port Activity LEDs will reflect the same traffic as the recipient port. Donor ports whose credits are being used are unavailable to devices that are connected to them.

5.4 Resetting a Port

The Reset Port option reinitializes the port using the saved configuration. To reset a port, do the following:

1. In the faceplate display, select the port(s) to be reset.
2. Open the Port menu and select **Reset Port**.

5.5 Testing Ports

The port loopback tests verify correct port operation by sending a frame out through the loop, and then verifying that the frame received matches the frame that was sent. Only one port can be tested at a time for each type of test. The Port Loopback Test dialog shown in Figure 5-4 presents the following loopback tests:

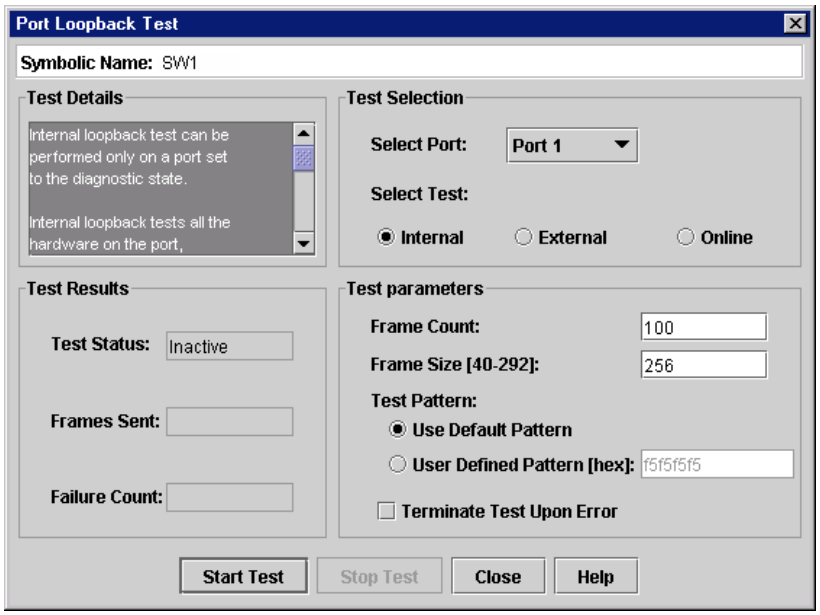


Figure 5-4. Port Loopback Test Dialog

- **SerDes level (Internal)** - The SerDes level test verifies port circuitry. The SerDes level test sends a test frame from the ASIC through the SerDes chip and back to the ASIC for the selected ports. The port passes the test if the frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.
- **SFP level (External)** - The SFP level test verifies port circuitry. The SFP level test sends a test frame from the ASIC through the SerDes chip, through the SFP transceiver fitted with an external loopback plug, and back to the ASIC for the selected ports. The port passes the test if the test frame that was sent by the ASIC matches the test frame that was received. This test requires that the port be in diagnostics mode, and therefore, disrupts communication.

- **Node-to-Node (Online)** - The Node-to-Node test verifies communications between the port and its device node or device loop. The port being tested must be online and connected to a remote device. The port passes the test if the frame that was sent by the ASIC matches the frame that was received. This test does not disrupt communication on the selected port. This test requires that the port be online, and therefore, does not disrupt communication.

To run the internal, external, or online port loopback test on a port, do the following:

1. In the faceplate display, select the port to be tested.
2. Open the Port menu and select **Port Loopback Test** to open the Port Loopback Test dialog.
3. In the Test Selection area, click the radio button for the type of loopback test to be run (Internal, External, or Online). If you choose the internal or external test, SANsurfer Switch Manager will prompt you to confirm that the port state needs to be changed to the diagnostic state. Click the **OK** button and SANsurfer Switch Manager will change the port state.
4. Enter the frame count, frame size, and click a test pattern radio button. You may use the default pattern or enter an 8-digit pattern (hex). For online test, you can check the **Terminate Test Upon Error** check box if you want the test to stop should it encounter an error.
5. Click the **Start Test** button to begin the test. The Test Results area displays the test status, number of frames sent, and number of errors found.
6. To test another port, open the Select Port pull-down menu and select another port (number) and test type (Internal, External, or Online) in the Test Selection area.
7. Click the **Start Test** button to begin the next test. Observe the results in the Test Results area.

5.6 Graphing Port Performance

SANsurfer Performance Viewer application displays port performance using graphs. SANsurfer Performance Viewer plots data communication rates and total errors for selected ports as shown in Figure 5-5. When graphing data communication rates, you can choose either frames/second or KB/second.

On Solaris platforms, if you launch the SANsurfer Performance Viewer application from the SANsurfer Switch Manager application and SANsurfer Performance Viewer can not connect to the fabric, (for example, if you have reached the maximum number of SANsurfer Switch Manager sessions on the entry switch), then SANsurfer Performance Viewer opens with a blue fabric icon displayed in the fabric tree.

Fabric status is displayed in text format after the fabric name in the fabric tree. The color of the icon indicates the current connection status as normal (green), warning (yellow), critical (red), or unmanageable (blue).

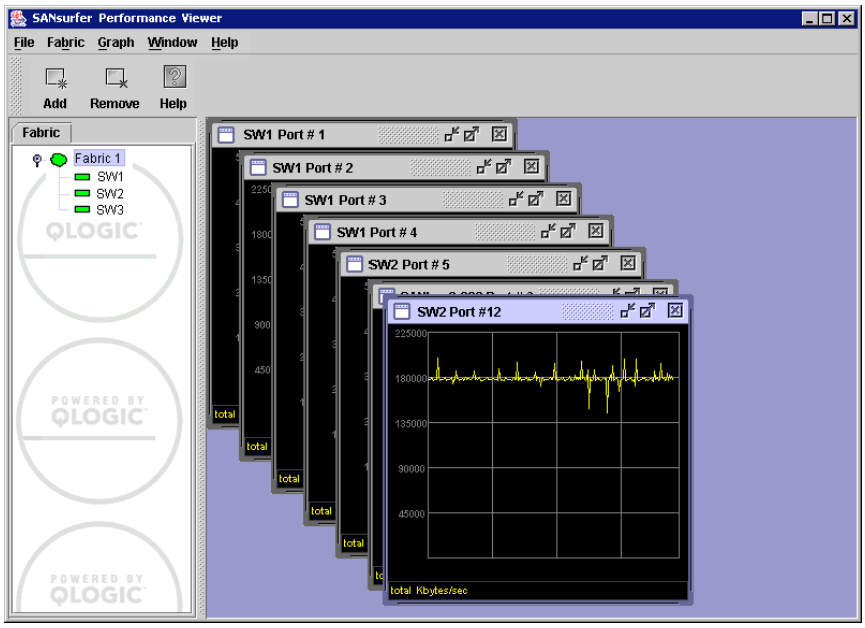


Figure 5-5. Fabric View Graphs

This section describes how to do the following:

- Starting SANsurfer Performance Viewer
- Exiting SANsurfer Performance Viewer
- Saving and Opening Performance View Files
- Changing the Default Performance View File Encryption Key
- Setting SANsurfer Performance Viewer Preferences
- Setting the Polling Frequency
- Displaying Graphs for a Switch
- Printing Graphs
- Saving Graph Statistics to a File

5.6.1 Starting SANsurfer Performance Viewer

To start SANsurfer Performance Viewer from within SANsurfer Switch Manager, open the topology display and select **Start Performance Viewer** from the Fabric menu. When starting the SANsurfer Performance Viewer application from the SANsurfer Switch Manager application on Linux and Solaris platforms, the fabric currently displayed in the SANsurfer Switch Manager topology display opens automatically in the SANsurfer Performance Viewer topology display. On Windows platforms, you will need to manually open the fabric in the SANsurfer Performance Viewer topology display.

Note: On the Solaris platforms, if you launch the SANsurfer Performance Viewer application from the SANsurfer Switch Manager application and SANsurfer Performance Viewer can not connect to the fabric, (for example, if you have reached the maximum number of SANsurfer Switch Manager sessions on the entry switch), then SANsurfer Performance Viewer opens with a blue fabric icon displayed in the fabric tree. The reason for status displayed after the fabric name in the fabric tree will indicate the reason for failure to connect.

5.6.2 Exiting SANsurfer Performance Viewer

To exit a SANsurfer Performance Viewer session, open the File menu and select **Exit**. The current fabric view is automatically saved to your default performance view file upon exit, if you have defined an encryption key. The key is encrypted and saved with your default performance view file. A performance view file contains the set of fabrics that have been added and the graphs that have been opened during a SANsurfer Performance Viewer session. If you have not yet defined an encryption key, the Save Default Performance View File dialog, shown

in Figure 5-6, prompts you to save the current performance view file as the default performance view file. Refer to ”Changing the Default Performance View File Encryption Key” on page 5-21 for information about defining and changing this encryption key.

In the Save Default Performance View File dialog, enter an encryption key in the Default Performance File Encryption Key field. Re-enter the encryption key in the Re-enter Encryption Key to Confirm field. Click the **OK** button to save the current set of fabrics to the default performance view file in the working directory.

To prevent SANsurfer Performance Viewer from prompting you to save the default performance view file between sessions, set the Auto Load and Save Graphing Environment setting to Enable (default). Refer to ”Setting SANsurfer Performance Viewer Preferences” on page 5-22 for more information.

Save Default Performance View File
An encryption key is required to encrypt information to be stored in a default performance view file when you exit the application.
Default File Encryption Key:
Re-enter Encryption Key to Confirm:
OK
Cancel
Help

Figure 5-6. Save Default Performance View File Dialog

In your next SANsurfer Performance Viewer session, the Load Default View File dialog shown in Figure 5-7 prompts you to load the default performance view file and to specify its encryption key, if there is one. In the Default Fabric File Encryption Key field, enter the encryption key and click the **Load View File** button. If you do not want to load the default performance view file, click the **Continue Without Loading** button to open the SANsurfer Performance Viewer with no fabric displayed.

Load Default View File
An encryption key is required to decrypt information stored in the default performance view file.
Default File Encryption Key:
Load View File
Continue Without Loading
Help

Figure 5-7. Load Default View File Dialog

5.6.3
Saving and Opening Performance View Files

In addition to the default performance view file, you can save and open your own performance view files. The performance view file contains the set of fabrics, graphs, and graphing options. To save a performance view file, do the following:

1. Open the File menu and select **Save View As** to open the Save View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file. Files are saved in the working directory.
3. Enter a password. When you attempt to open this fabric file, you will be prompted for this password. If you leave the File Password field blank, no password is required.

To open a performance view file, do the following:

1. Open the File menu and select **Open View File** to open the Open View dialog.
2. Enter a name for the fabric file or click the **Browse** button to select an existing file.

5.6.4
Changing the Default Performance View File Encryption Key

To change the encryption key for the default performance view file, do the following:

1. Open the File menu and select **Save Default Performance View File** to open the Save Default Performance View File dialog.
2. Enter the new encryption key in the Default File Encryption Key field.
3. Re-enter the same encryption key in the Re-enter Encryption Key to Confirm field.
4. Click the **OK** button to save the changes.

5.6.5
Setting SANsurfer Performance Viewer Preferences

To set preferences, open the File menu and select **Preferences** to open the Preferences dialog shown in Figure 5-8. Set the following preferences and click the **OK** button to save the changes:

- Change the location of the working directory in which to save files
- Change the location of the browser used to view the online help.
- Enable or disable the **Auto Load and Auto Save Graphing Options** preference. When enabled, SANsurfer Performance Viewer prompts you to save and load the default fabric file between sessions. Refer to "Exiting SANsurfer Performance Viewer" on page 5-19 for more information on the default performance view file.
- Enable or disable the Display Dialog When Making Non-secure Connections checkbox. If enabled, the Non-secure Connections Check dialog is displayed when you attempt to open a non-secure fabric. You then have the option of opening a non-secure fabric. If disabled, you cannot open a fabric with a non-secure connection).

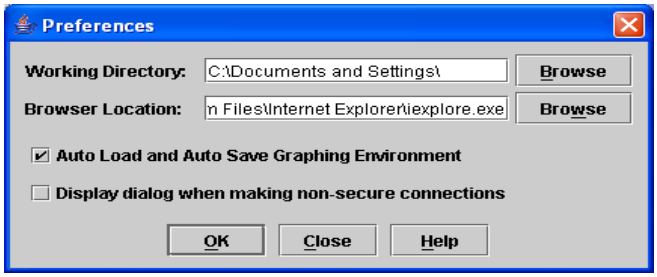


Figure 5-8. Preferences – SANsurfer Performance Viewer

5.6.6
Setting the Polling Frequency

SANsurfer Performance Viewer updates the graphs once per second by default. To change this polling frequency, do the following:

1. Open the Graph menu, and select **Set Polling Frequency** to open the Set Graph Polling Frequency dialog.
2. Enter the new polling interval in seconds [1–60]. Performance Viewer will update the graphs once during the interval. For example, setting the polling frequency to 5 seconds will return 1 second's worth of data every 5 seconds.
3. Click the **OK** button to save the changes.

5.6.7
Displaying Graphs for a Switch

To display graphs, do the following:

1. Open the Fabric menu and select **Add Fabric** or click the **Add** button. Enter a fabric name and an IP address in the Add a New Fabric dialog. Include an account name and a password if required.
2. Set the graphing options and polling frequency. By default, SANsurfer Performance Viewer plots total bytes transmitted and received at a polling frequency of once per second. Refer to ”Customizing Graphs” on page 5-24 for information about changing what is plotted and how it is plotted.
3. You can display graphs in the following ways:
   - Click on a switch entry handle and select one or more ports.
   - Right click on a switch icon in the fabric tree and select **Open Graph for All Ports on Switch** or **Open Graph for All Logged-In Ports on Switch** from the pull-down menu.
4. You can move graphs around individually by clicking and dragging, or you can arrange them as a group. Refer to ”Arranging Graphs in the Display” on page 5-24 for more information.

To remove a graph, click the graph **Remove** button. To remove all graphs, open the Window menu and select **Close All**.

To remove a fabric and its graphs, select the fabric in the fabric tree, then select **Remove Fabric** from the Fabric menu. You can also right click on a fabric and select **Remove Fabric** for the popup menu.

Right clicking on a graph opens a popup menu from which you can change graph options, print a graph, or save the graph statistics to a file.

5.6.7.1
Displaying Graphs for a Stack

The switch management application recognizes switches as a stack if they are connected by their high speed stacking ports (10-Gbps switches only). The switch management application will auto-detect such switches connected by their 10-Gbps ports and will display these stacked switches as a single stack entity in the topology and faceplate displays.

Graphs can be displayed for all ports on all switches in a stack or for only those ports on all switches that are logged in. To display graphs for stacks, do the following:

1. In the left-pane/fabric tree, right-click on a Stack icon.
2. In the popup menu, select **Open Graph For All Ports on Stack** or **Open Graph For All Logged-In Ports on Stack**.

5.6.7.2
Arranging Graphs in the Display

To arrange and size graphs in the display, open the Window menu and select **Cascade**, **Tile**, or **Close All**.

- **Cascade** overlaps the graphs so that all graphs are at least partially visible.
- **Tile** arranges the graphs in non-overlapping rows and columns.
- **Close All** closes all graphs.

You can also click a graph on the Window menu to bring that graph to the front.

5.6.7.3
Customizing Graphs

You can customize the graph polling frequency, what is plotted in the graphs, and the graph color scheme. To set the polling frequency for all graphs, open the Graph menu and select **Set Polling Frequency...**. Enter an interval in seconds (0–60) in the dialog box and click the **OK** button.

To choose what is to be plotted, open the Graph menu and select **Modify Graph Options...**. You can also right click on a graph and select **Change Graph Options**. This opens the Default Graph Options dialog shown in Figure 5-9.

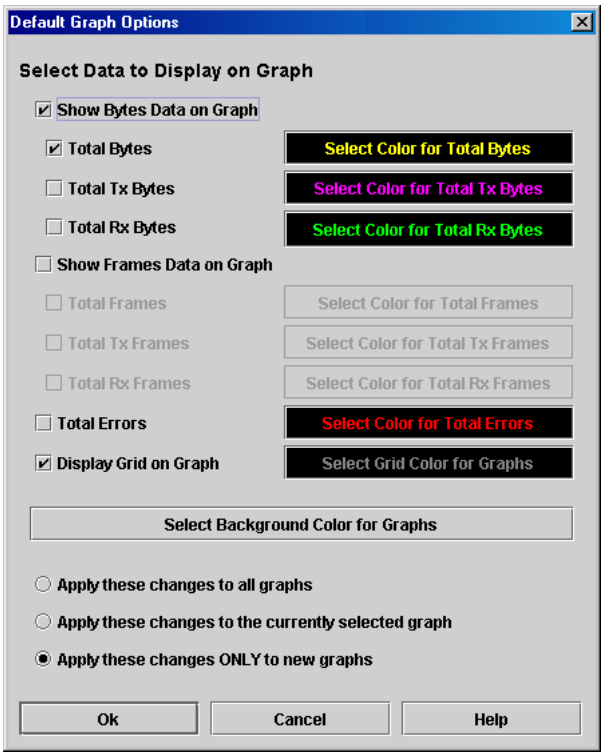

Default Graph Options
Select Data to Display on Graph
Show Bytes Data on Graph
Total Bytes
Select Color for Total Bytes
Total Tx Bytes
Select Color for Total Tx Bytes
Total Rx Bytes
Select Color for Total Rx Bytes
Show Frames Data on Graph
Total Frames
Select Color for Total Frames
Total Tx Frames
Select Color for Total Tx Frames
Total Rx Frames
Select Color for Total Rx Frames
Total Errors
Select Color for Total Errors
Display Grid on Graph
Select Grid Color for Graphs
Select Background Color for Graphs
Apply these changes to all graphs
Apply these changes to the currently selected graph
Apply these changes ONLY to new graphs
Ok
Cancel
Help

Figure 5-9. Default Graph Options Dialog

To modify the graph options, do the following:

1. Choose the units for the graph:
   - Select the **Show Bytes Data on Graph** check box to plot data in KBytes/second
   - Select the **Show Frames Data on Graph** check box to plot data in frames/second.
2. Choose what data type to plot. For example, if you selected **Show Frames Data on Graph** in step 1., you can plot one or all of the following:
   - Total frames transmitted and received (**Total Frames**)
   - Total frames transmitted (**Total Tx Frames**)
   - Total frames received (**Total Rx Frames**)

   In addition to these, you can also plot total errors by selecting the **Total Errors** check box.
3. Display or hide the unit grid. Select the **Display Grid on Graph** check box to display the unit grid.
4. Choose the color scheme for the graph. Click a **Select Color** button to open its corresponding Select Color dialog, which allows you to select a new color scheme. You can select the color for each data type, the unit grid, and the background by clicking the corresponding color field or button. In each case, you can choose a color using the Swatches, Red-Green-Blue (RGB), or Hue-Saturation-Brightness (HSB) method.

   Note: Clicking the **Reset** button in the Swatches, HSB, and RGB tab pages of the Select Color dialogs will reset the colors in the Preview area to the last saved color scheme. At this point you are only selecting a new color scheme to be saved.

   - Swatches – Click the **Swatches** tab. Select a swatch from the palette.
   - HSB – Click the **HSB** tab. Select a color using the following methods:
     - Click in the color palette.
     - Select the **H**, **S**, or **B** button and use the slide to vary the value.
     - Enter values in the H, S, or B input fields.
   - RGB – Click the **RGB** tab. Select a color by moving the slides to adjust the values for red, blue, and green; or enter values in the input fields.
5. In the Default Graph Options dialog, click the corresponding radio button to apply changes to all graphs, the currently selected graph, or all new graphs.
6. In the Default Graph Options dialog, click the **OK** button to save the color scheme changes and close the dialog.

5.6.7.4
Setting Global Graph Type

The Set Global Graph Type option enables you to view port activity using two types of graphs:

- Line Graph - plots continuous port activity in horizontal line format.
- Bar Graph - the last polling value received by the application in bar graph format.

To set the global graph type, open the Graph menu and select **Line Bar** or **Bar Graph**.

5.6.7.5
Rescaling a Selected Graph

The Rescale Selected Graph option auto-scales downward and re-positions the data within a graphic window to display all new data captured by the graph. To rescale a selected graph, do the following:

1. Select a displayed graph.
2. Open the Graph menu and select **Rescale Selected Graph**, or right-click on the graph and select **Rescale** from the popup menu.
3. View the data in the graph window.

5.6.8
Printing Graphs

To print a graph, select a graph, then open the File menu and select **Print Graph Window**. You can also right click on a graph and select **Print Graph Window** from the popup menu.

5.6.9
Saving Graph Statistics to a File

Statistics for one or all graphs can be saved to a file that can be opened with a spreadsheet application. To save a graph statistics file, do the following:

1. Select a graph.
2. Open the File menu, and select **Save Current Graph Statistics to a File** to save the selected graph or select **Save All Graph Statistics to a File**. You can also right click on a graph and select **Save Statistics to File**.
3. In the Save dialog, enter a path name for the file. By default, the file is saved in the working directory.
4. Click the **Save** button.

Appendix A

Command Line Interface

- Logging On to a Switch
- User Accounts
- Working with Switch Configurations
- Commands

A.1 Logging On to a Switch

To log on to a switch using Telnet, open a command line window on the workstation and enter the Telnet command followed by the switch IP address:

```
# telnet ip_address
```

A Telnet window opens prompting you for a login. Enter an account name and password.

To log on to a switch through the serial port, configure the workstation port with the following settings:

- 9600 baud
- 8-bit character
- 1 stop bit
- No parity

Enter an account name and password when prompted.

A.2 User Accounts

Switches come from the factory with the following user account already defined:

Account name: admin
Password: password
Authority: Admin

This user account provides full access to the switch and its configuration. After planning your fabric management needs and creating your own user accounts, consider changing the password for this account.

- Refer to ”Commands” on page A-6 for information about authority levels.
- Refer to the ”User Command” on page A-123 for information about creating user accounts.
- Refer to ”Passwd Command” on page A-41 for information about changing passwords.

Note: A switch supports a combined maximum of 19 logins or sessions reserved as follows:

- 4 logins or sessions for internal applications such as management server and SNMP
- 9 high priority Telnet sessions
- 6 logins or sessions for SANsurfer Switch Manager inband and out-of-band logins, Application Programming Interface (API) inband and out-of-band logins, and Telnet logins. Additional logins will be refused.

A.3 Working with Switch Configurations

Successful management of switches and fabrics with the command line interface depends on the effective use of switch configurations. Modifying configurations, backing up configurations, and restoring configurations are key switch management tasks.

A.3.1
Modifying a Configuration

A switch supports up to 10 configurations including the default configuration. Each switch configuration contains switch, port, port threshold alarm, and zoning configuration components. The Show Switch command displays the name of the active configuration. A configuration name can have up to 31 characters excluding the pound symbol (#), semicolon (;), and comma (,). By editing the latest configuration and saving the results under a new name, you can create a history of configuration changes. Use the Config List command to display the configurations stored on the switch

```
SANbox Manager #> config list
  Current list of configurations
  ------------------------------
  default
  config_10132003
```

To modify a switch configuration you must open an Admin session with the Admin Start command. An Admin session prevents other accounts from making changes at the same time either through Telnet or SANsurfer Switch Manager. You must also open a Config Edit session with the Config Edit command and indicate which configuration you want to modify. If you do not specify a configuration name the active configuration is assumed. The Config Edit session provides access to the Set Config commands with which you make modifications to the port, switch, port threshold alarm, or zoning configuration components as shown:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config edit default
   The config named default is being edited.
SANbox Manager (admin-config)#> set config port . . .
SANbox Manager (admin-config)#> set config switch . . .
SANbox Manager (admin-config)#> set config threshold . . .
SANbox Manager (admin-config)#> set config zoning . . .
```

The Config Save command saves the changes you made during the Config Edit session. In this case, changes to the configuration named *Default* are being saved to a new configuration named *config_10132003*. However, the new configuration does not take effect until you activate it with the Config Activate command:

```
SANbox Manager (admin-config)#> config save config_10132003
SANbox Manager (admin)#> config activate config_10132003
SANbox Manager (admin)#> admin end
```

The Admin End command releases the Admin session for other administrators when you are done making changes to the switch.

A.3.2
Backing up and Restoring Switch Configurations

Backing up and restoring a configuration is useful to protect your work or for use as a template in configuring other switches. The Config Backup command creates a file on the switch, named *configdata*. This file can be used to restore a switch configuration only from the command line interface; it cannot be used to restore a switch using SANsurfer Switch Manager.

```
SANbox Manager  #> admin start
SANbox Manager (admin) #> config backup
```

The *configdata* file contains all of the switch configuration information including the following:

- All named switch configurations including the default configuration. This includes port, switch, port threshold alarm, and zoning configuration components.
- All SNMP and network information defined with the Set Setup command.
- The zoning database included all zone sets, zones, and aliases

You use FTP to download the *configdata* file to your workstation for safe keeping and to upload the file back to the switch for the restore function. To download the configdata file, open an FTP session on the switch and login with the account name *images* and password *images*. Transfer the file in binary mode with the Get command as shown:

```
>ftp ip_address
user:images
password: images

ftp>bin
ftp>get configdata
    xxxxx bytes sent in xx secs.
ftp>quit
```

You should rename the *configdata* file on your workstation with the switch name and date, *config_switch_169_10112003*, for example.

The restore operation begins with FTP to upload the configuration file from the workstation to the switch, then finishes with a Telnet session and the Config Restore command. To upload the configuration file, *config_switch_169_10112003* in this case, open and FTP session with account name *images* and password *images*. Transfer the file in binary mode with the Put command as shown:

```
ftp ip_address
user:images
password: images
ftp> bin
ftp> put config_switch_169_10112003 configdata
  Local file config_switch_169_10112003
  Remote file configdata
ftp>quit
```

The restore process replaces all configuration information on the switch and afterwards the switch is automatically reset. If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the ”Set Setup Command” on page A-81. To restore the switch, open a Telnet session, then enter the Config Restore command from within an Admin session as shown:

```
SANbox Manager  #> admin start
SANbox Manager (admin) #> config restore
  The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
```

A.4 Commands

The command syntax is as follows:

command
keyword
keyword *[value]*
keyword [value1] [value2]

The **Command** is followed by one or more keywords. Consider the following rules and conventions:

- Commands and keywords are case insensitive.
- Required keyword values appear in standard font: [value]. Optional values are shown in italics: *[value].*
- Underlined portions of the keyword in the command format indicate the abbreviated form that can be used. For example the Delete keyword can be abbreviated Del.

The command-line completion feature makes entering and repeating commands easier. Table A-1 describes the command-line completion keystrokes.

Table A-1. Command-Line Completion

Keystroke	Effect
Tab	Completes the command line. Enter at least one character and press the tab key to complete the command line. If more than one possibility exists, press the Tab key again to display all possibilities.
Up Arrow	Scrolls backward through the list of previously entered commands.
Down Arrow	Scrolls forward through the list of previously entered commands.
Control-A	Moves the cursor to the beginning of the command line
Control-E	Moves the cursor to the end of the command line.

The command set performs monitoring and configuration tasks. Commands related to monitoring tasks are available to all account names. Commands related to configuration tasks are available only within an admin session. An account must have Admin authority to enter the Admin Start command, which opens an admin session. Refer to the ”Admin Command” on page A-8.

The commands and their page numbers are listed in Table A-2.

Table A-2. Commands Listed by Authority Level

Monitoring Commands		Configuration Command	
Help	(A-34)	Admin	(A-8)
History	(A-35)	**Admin Session Commands**	
Ping	(A-42)		
Ps	(A-43)	Alias[1]	(A-9)
Quit	(A-44)	CIM[1]	(A-11)
Show	(A-91)	CIMListener	(A-12)
Show Config	(A-106)	CIMSubscription	(A-14)
Show Log	(A-109)	Config[1]	(A-16)
Show Perf	(A-112)	Create	(A-19)
Show Setup	(A-114)	Date[1]	(A-22)
Uptime	(A-122)	Feature[1]	(A-23)
Whoami	(A-126)	Firmware Install	(A-23)
		Group[1]	(A-25)
		Hardreset	(A-33)
		Hotreset	(A-36)
		Image	(A-37)
		Lip	(A-40)
		Passwd	(A-41)
		Reset	(A-45)
		Security	(A-53)
		Securityset[1]	(A-57)
		Set[1]	(A-59)
		Set Config	(A-61)
		Set Log	(A-75)
		Set Port[1]	(A-79)
		Set Setup	(A-81)
		Shutdown	(A-118)
		Test	(A-119)
		User[1] [2]	(A-123)
		Zone[1]	(A-127)
		Zoneset[1]	(A-131)
		Zoning[1]	(A-133)

[1]Some keywords do not require an Admin session.

[2] Some keywords can be executed only by the Admin account name.

Admin Command

Opens and closes an Admin session. The Admin session provides commands that change the fabric and switch configurations. Only one Admin session can be open on the switch at any time. An inactive Admin session will time out after a period of time which can be changed using the Set Setup System command. Refer to the ”Set Setup Command” on page A-81.

Authority Admin

Syntax **admin**
start (or begin)
end (or stop)
cancel

Keywords **start (or begin)**
Opens the admin session.

end (or stop)
Closes the admin session. The Hardreset, Hotreset, Logout, Shutdown, and Reset Switch commands will also end an admin session.

cancel
Terminates an Admin session opened by another user. Use this keyword with care because it terminates the Admin session without warning the other user and without saving pending changes.

Notes Closing a Telnet window during an admin session does not release the session. In this case, you must either wait for the admin session to time out, or use the Admin Cancel command.

Examples The following example shows how to open and close an Admin session:

```
SANbox Manager #> admin start

SANbox Manager (admin) #>

.
.
.

SANbox Manager (admin) #> admin end
SANbox Manager #>
```

Alias Command

Creates a named set of ports/devices. Aliases make it easier to assign a set of ports/devices to many zones. An alias can not have a zone or another alias as a member.

Authority Admin session for all keywords except List and Members

Syntax **alias**

add [alias] [member_list]
copy [alias_source] [alias_destination]
create [alias]
delete [alias]
list
members [alias]
remove [alias] [member_list]
rename [alias_old] [alias_new]

Keywords

add [alias] [member_list]
Specifies one or more ports/devices given by [member_list] to add to the alias named [alias]. Use a <space> to delimit ports/devices in [member_list]. An alias can have a maximum of 2000 members. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.

The application verifies that the [alias] format is correct, but does not validate that such a port/device exists.

copy [alias_source] [alias_destination]
Creates a new alias named [alias_destination] and copies the membership into it from the alias given by [alias_source].

create [alias]
Creates an alias with the name given by [alias]. An alias name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 aliases.

delete [alias]
Deletes the specified alias given by [alias] from the zoning database. If the alias is a member of the active zone set, the alias will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all aliases. This keyword does not require an admin session.

members [alias]
Displays all members of the alias given by [alias]. This keyword does not require an admin session.

remove [alias] [member_list]
Removes the ports/devices given by [member_list] from the alias given by [alias]. Use a <space> to delimit ports/devices in [member_list]. A port/device in [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) for the device with the format xx:xx:xx:xx:xx:xx:xx:xx.

rename [alias_old] [alias_new]
Renames the alias given by [alias_old] to the alias given by [alias_new].

CIM Command

Manages CIM listener and subscription configurations on the switch. Refer to the "CIMListener Command" on page A-12 for information about creating and modifying CIM listeners. Refer to the "CIMSubscription Command" on page A-14 for information about creating and modifying CIM subscriptions.

Authority Admin session

Syntax

cim
- cancel
- clear
- edit
- limits
- save

Keywords

cancel
Terminates the current CIM edit session without saving changes that were made.

clear
Clears all CIM listener and subscription configurations from the switch.

edit
Opens a CIM edit session.

limits
Displays the maximum allowed number of CIM listeners, subscriptions, and subscriptions per listener. This keyword does not require an Admin session nor a CIM edit session.

save
Saves all changes made during the current CIM edit session.

Examples The following is an example of the CIM Edit command:

```
SANbox Manager (admin) #> cim edit
SANbox Manager (admin-cim) #> cimlistener create CIM_listener_1
.
.
.
SANbox Manager (admin-cim) #> cim save
```

The following is an example of the CIM Limits command:

```
SANbox Manager #> cim limits

  Cim Attribute                Maximum
  -------------                -------
  MaxListeners                 32
  MaxSubscriptions             50
  MaxSubscriptionsPerListener  6
```

CIMListener Command

Configures CIM indication service listeners and adds subscriptions to listeners. Refer to the ”CIMSubscription Command” on page A-14 for information about configuring subscriptions.

Authority Admin session and a CIM Edit session. Refer to the ”CIM Command” on page A-11 for information about opening a CIM edit session.

Syntax

cimlistener
add [listener_name] [subscription_list]
create [listener_name]
delete [listener_name]
edit [listener_name]

Keywords

add [listener_name] [subscription_list]
Adds the set of subscriptions given by [subscription_list] to the listener given by [listener_name]. Use a <space> to delimit subscription names in [subscription_list].

create [listener_name]
Prompts you in a line-by-line fashion to create a CIM listener with the name given by [listener_name]. [listener_name] can have up to 32 characters: 0-9, A-Z, a-z, _, $, ^, and -. The CIM listener configuration parameters are described in Table A-3.

Table A-3. CIM Listener Configuration Parameters

Parameter	Description
Name	Listener name
Type	Listener type: ■ Permanent – Send indications to the CIM client whether a connection can be established or not. This is the default. ■ Transient – Sends indications to the CIM client, but ceases if a connection cannot be established after 60 minutes.
URL	IP address of the CIM client and the port number to which to send indications. The default is 10.0.0.1:5000.

delete [listener_name]
Deletes the listener given by [listener_name] from the CIM database.

edit [listener_name]
Opens an editing session in which you can modify the CIM listener given by [listener_name]. Refer to Table A-3 for a description of the CIM listener configuration parameters.

Examples

The following is an example of the CIMListener Create command:

```
SB5602-91.54 (admin-cim) #> cimlistener create listener_1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Name  listener_1
  Type  (2=Permanent, 3=Transient)   [Permanent    ]
  URL   (IP address:port format)     [10.0.0.1:5000]

  Finished configuring attributes.
  This configuration must be saved with the cim save command
  before it can take effect, or to discard this configuration
  use the cim cancel command.
```

CIMSubscription Command

Creates, edits, or removes CIM subscriptions.

Authority Admin session and a CIM Edit session. Refer to the ”CIM Command” on page A-11 for information about opening a CIM edit session.

Syntax

cimsubscription
create [subscription_name]
delete [subscription_name]
edit [subscription_name]

Keywords

create [subscription_name]
Prompts you in a line-by-line fashion to create a CIM subscription with the name given by [subscription_name]. [subscription_name] can have up to 32 characters: 0-9, A-Z, a-z, _, $, ^, and -. Table A-4 describes the CIM subscription configuration parameters.

Table A-4. CIM Subscription Configuration Parameters

Parameter	Description
Name	Subscription name.
FilterID	Event type for which the switch monitors and sends an indication to the CIM client. The event types are as follows: ■ CreateComputerSystem – A switch is added to the fabric. This is the default. ■ ModifyComputerSystem – A switch state change. ■ DeleteComputerSystem – A switch is removed from the fabric. ■ CreateFCPort – Not supported. ■ ModifyFCPort – A Fibre Channel port state change. ■ DeleteFCPort – Not supported.
EnabledState	Enable (True) or disable (False) the subscription. The default is True.
Duration	Subscription life span in seconds. The subscription life span begins when the subscription is created. Expired subscriptions do not send indications to the CIM client though they remain in the CIM database. Values can be 1–720000. 0 indicates indefinite, which is the default.

delete [subscription_name]
Deletes the subscription given by [subscription_name] from the CIM database.

edit [subscription_name]
Opens an editing session in which you can modify the CIM subscription given by [subscription_name]. Refer to Table A-4 for a description of the CIM subscription configuration parameters.

Examples

The following is an example of the CIMSubscription Create command:

```
SANbox Manager (admin-cim) #> cimsubscription create subscription_1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

     FilterID values:  1 = Create:ComputerSystem
                       2 = Modify:ComputerSystem
                       3 = Delete:ComputerSystem
                       4 = Create:FCPort
                       5 = Modify:FCPort
                       6 = Delete:FCPort

  Name          subscription_1
  FilterID      (see allowed options above)               [Create:ComputerSystem]
  EnabledState  (True / False)                            [True                 ]
  Duration      (decimal value, 0-720000 secs, 0=forever) [0                    ]

  Finished configuring attributes.
  This configuration must be saved with the cim save command
  before it can take effect, or to discard this configuration
  use the cim cancel command.
```

Config Command

Manages the Fibre Channel configurations on a switch. For information about setting the port and switch configurations, refer to the ”Set Config Command” on page A-61.

Authority Admin session for all keywords except List

Syntax

config
activate *[config_name]*
backup
cancel
copy [config_source] [config_destination]
delete [config_name]
edit *[config_name]*
list
restore
save *[config_name]*

Keywords

activate *[config_name]*
Activates the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used. Only one configuration can be active at a time.

backup
Creates a file named *configdata*, which contains the system configuration information. To download this file, open an FTP session, log in with account name/password of “images” for both, and type “get configdata”. Refer to ”Backing up and Restoring Switch Configurations” on page A-4.

cancel
Terminates the current configuration edit session without saving changes that were made.

copy [config_source] [config_destination]
Copies the configuration given by [config_source] to the configuration given by [config_destination]. The switch supports up to 10 configurations including the default configuration.

delete [config_name]
Deletes the configuration given by [config_name] from the switch. You cannot delete the default configuration (Default Config) nor the active configuration.

edit *[config_name]*
Opens an edit session for the configuration given by [config_name]. If you omit [config_name], the currently active configuration is used.

list
Displays a list of all available configurations on the switch. This keyword does not require an admin session.

restore
Restores configuration settings to an out-of-band switch from a backup file named *configdata*, which must be first uploaded on the switch using FTP. You create the backup file using the Config Backup command. Use FTP to load the backup file on a switch, then enter the Config Restore command. After the restore is complete, the switch automatically resets. Refer to ”Backing up and Restoring Switch Configurations” on page A-4.

Note:
- If the restore process changes the IP address, all management sessions are terminated. Use the Set Setup System command to return the IP configuration to the values you want. Refer to the ”Set Setup Command” on page A-81.
- Configuration archive files created with the SANsurfer Switch Manager Archive function are not compatible with the Config Restore command.

save *[config_name]*
Saves changes made during a configuration edit session in the configuration given by [config_name]. If you omit [config_name], the value for [config_name] you chose for the most recent Config Edit command is used. [config_name] can be up to 31 characters excluding #, semicolon (;), and comma (,). The switch supports up to 10 configurations including the default configuration.

Notes

If you edit the active configuration, changes will be held in suspense until you reactivate the configuration or activate another configuration.

Examples

The following shows an example of how to open and close a Config Edit session:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config edit
   The config named default is being edited.
.
.
SANbox Manager (admin-config) #> config cancel
  Configuration mode will be canceled. Please confirm (y/n): [n] y
SANbox Manager (admin) #> admin end
```

The following is an example of how to create a backup file (configdata) and download the file to the workstation.

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config backup
SANbox Manager (admin) #> admin end
SANbox Manager #> exit

#>ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> get configdata
ftp> quit
```

The following is an example of how to upload a configuration backup file (configdata) from the workstation to the switch, and then restore the configuration.

```
#> ftp symbolic_name or ip_address
user: images
password: images
ftp> bin
ftp> put configdata
ftp> quit

SANbox Manager #> admin start


SANbox Manager (admin) #> config restore
The switch will be reset after restoring the configuration.
  Please confirm (y/n): [n] y
  Alarm Msg: [day month date time year][A1005.0021][SM][Configuration is being
restored -  this could take several minutes !]
  Alarm Msg: [day month date time year][A1000.000A][SM][The switch will be reset in
3 seconds due to a config restore]
SANbox Manager (admin) #>
  Alarm Msg: [day month date time year][A1000.0005][SM][The switch is being reset]
Good bye.
```

Create Command

Creates support files for troubleshooting switch problems, and certificates for secure communications for SANsurfer Switch Manager.

Authority Admin session

Syntax

create
certificate
support

Keywords

certificate

Creates a security certificate on the switch. The security certificate is required to establish an SSL connection with a management application such as SANsurfer Switch Manager. The certificate is valid 24 hours before the certificate creation date and expires 365 days after the creation date. Should the current certificate become invalid, use the Create Certificate command to create a new one.

Note: To insure the creation of a valid certificate, be sure that the switch and the workstation time and date are the same. Refer to the following:

- ”Date Command” on page A-22 for information about setting the time and date
- ”Set Command” on page A-59 (Timezone keyword) for information about setting the time zone on the switch and workstation
- ”Set Setup Command” on page A-81 (System keyword) for information about enabling the Network Time Protocol for synchronizing the time and date on the switch and workstation from an NTP server.

support

Assembles all log files and switch memory data into a core dump file (dump_support.tgz) on the switch. If your workstation has an FTP server, you can proceed with the command prompts to send the file from the switch to a remote host. Otherwise, you can use FTP to download the support file from the switch to your workstation. The support file is useful to technical support personnel for troubleshooting switch problems. Use this command when directed by your authorized maintenance provider.

Examples

The following is an example of the Create Support command when an FTP server is available on the workstation:

```
SANbox Manager (admin) #> create support

Log Msg:[Creating the support file - this will take several seconds]

FTP the dump support file to another machine? (y/n): y

Enter IP Address of remote computer: 10.20.33.130

Login name: johndoe

Enter remote directory name: bin/support

Would you like to continue downloading support file? (y/n) [n]: y

Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.

Password:  xxxxxxx


230 User johndoe logged in.
cd bin/support
250 CWD command successful.

lcd /itasca/conf/images

Local directory now /itasca/conf/images

bin

200 Type set to I.
put dump_support.tgz
local: dump_support.tgz remote: dump_support.tgz
227 Entering Passive Mode (10,20,33,130,232,133)
150 Opening BINARY mode data connection for dump_support.tgz.
226 Transfer complete.
43430 bytes sent in 0.292 secs (1.5e+02 Kbytes/sec)
Remote system type is UNIX.
Using binary mode to transfer files.
221-You have transferred 43430 bytes in 1 files.
221-Total traffic for this session was 43888 bytes in 1 transfers.
221 Thank you for using the FTP service on localhost.localdomain.
```

The following is an example of the Create Support command and how to download the support file to your workstation. When prompted to send the support file to another machine, decline, then close the Telnet session. Open an FTP session on the switch and log in with the account name *images* and password *images*. Transfer the dump_support.tgz file in binary mode with the Get command.

```
SANbox Manager (admin) #> create support
Log Msg:[Creating the support file - this will take several seconds]
FTP the dump support file to another machine? (y/n): n

SANbox Manager (admin) #> quit
>ftp switch_ip_address
user:     images
password: images

ftp>bin
ftp>get dump_support.tgz
    xxxxx bytes sent in xx secs.
ftp>quit
```

The following is an example of the Create Certificate command:

```
SANbox Manager (admin) #> create certificate
  The current date and time is day mon date hh:mm:ss UTC yyyy.
  This is the time used to stamp onto the certificate.
  Is the date and time correct? (y/n): [n] y
  Certificate generation successful.
```

Date Command

This command displays or sets the system date and time. To set the date and time the information string must be provided in this format: MMDDhhmmCCYY. The new date and time takes effect immediately.

Authority Admin session except to display the date.

Syntax **date**
[MMDDhhmmCCYY]

Keywords ***[MMDDhhmmCCYY]***
Specifies the date – this requires an admin session. If you omit [MMDDhhmmCCYY], the current date is displayed which does not require an admin session.

Notes Network Time Protocol (NTP) must be disabled to set the time with the Date command. Refer to the ”Set Setup Command” on page A-81, System keyword, for information about NTP.

When setting the date and time on a switch that is enabled for SSL connections, the switch time must be within 24 hours of the workstation time. Otherwise, the connection will fail.

Examples The following is an example of the Date command:

```
SANbox Manager #> date
  Mon Apr 07 07:51:24 2003
```

Feature Command

Adds license key features to the switch and displays the license key feature log. To order a license key contact your switch distributor or your authorized reseller. Upgrading a switch is not disruptive, nor does it require a switch reset.

Authority Admin session for Add keyword only

Syntax **feature**
add [license_key]
log

Keywords **add [license_key]**
Adds the feature that corresponds to the value given by [license_key]. [license_key] is case insensitive.

log
Displays a list of installed license key features.

NotesFirmware Install Command

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch (without a power-on self test) to activate the firmware. If possible, a non-disruptive activation is performed. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

Authority Admin

Syntax **firmware install**

Examples The following is an example of the Firmware Install command:

```
SANbox Manager (admin) #> firmware install
 Warning: Installing new firmware requires a switch reset.
 A stable farbic is required to successfully activate the firmware on a
 switch without disrupting traffic. Therefore, before continuing with
 this action, ensure there are no administrative changes in progress
 anywhere in the fabric.
 Continuing with this action will terminate all management sessions,
 including any Telnet sessions. When the firmware activation is complete,
 you may log in to the switch again.

 Do you want to continue? [y/n]: y
    Press 'q' and the ENTER key to abort this command.
  User Account    : johndoe
  IP Address      : 10.20.33.130
```

```
  About to install image.  Do you want to continue? [y/n] y
Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Group Command

Creates groups, manages membership within the group, and manages the membership of groups in security sets.

Authority Admin session and a Security Edit session. Refer to the ”Security Command” on page A-53 for information about starting a Security Edit session. The List, Members, Securitysets, and Type keywords are available without an Admin session.

Syntax **group**

add [group]
copy
create [group] *[type]*
delete [group]
edit [group] [member]
list
members [group]
remove [group] [member_list]
rename [group_old] [group_new]
securitysets [group]
type [group]

Keywords

add [group]

Initiates an editing session in which to specify a group member and its attributes for the existing group given by [group]. ISL, Port, and MS member attributes are described in Table A-5, Table A-6, and Table A-7 respectively. The group name and group type attributes are read-only fields common to all three tables.

Table A-5. ISL Group Member Attributes

Attribute	Description
Member	Worldwide name of the switch that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the ISL member. The hash functions are MD5 or SHA-1. If the ISL member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the ISL group member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the ISL group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the ISL group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Binding	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the ”Set Config Command” on page A-61. 0 (zero) specifies no binding.

Table A-6. Port Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch. A member cannot belong to more than one group.
Authentication	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP). The default is None.
Primary Hash	The preferred hash function to use to decipher the encrypted Primary Secret sent by the Port group member. The hash functions are MD5 or SHA-1. If the Port group member does not support the Primary Hash, the switch will use the Secondary Hash.
Primary Secret	Hexadecimal string that is encrypted by the Primary Hash for authentication with the Port group member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash	Hash function to use to decipher the encrypted Secondary Secret sent by the Port group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the Port group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

Table A-7. MS Group Member Attributes

Attribute	Description
Member	Port worldwide name for the N_Port device that would attach to the switch.
CTAuthentication	Common Transport (CT) authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Hash	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Secret	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

copy [group_source] [group_destination]
Creates a new group named [group_destination] and copies the membership into it from the group given by [group_source].

create [group] ***[type]***
Creates a group with the name given by [group] with the type given by [type]. A group name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 16 groups. If you omit [type], ISL is used. [type] can be one of the following:

ISL
Configures security for attachments to other switches.

Port
Configures security for attachments to N_Port devices.

MS
Configures security for attachments to N_Port devices that are issuing management server commands.

edit [group] [member]
Initiates an editing session in which to change the attributes of a worldwide name given by [member] in a group given by [group]. Member attributes that can be changed are described in Table A-8:

Table A-8. Group Member Attributes

Attribute	Description
Authentication (ISL and Port Groups)	Enables (CHAP) or disables (None) authentication using the Challenge Handshake Authentication Protocol (CHAP).
CTAuthentication (MS Groups)	CT authentication. Enables (True) or disables (False) authentication for MS group members. The default is False.
Primary Hash (ISL and Port Groups)	The preferred hash function to use to decipher the encrypted Primary Secret sent by the member. The hash functions are MD5 or SHA-1. If the member does not support the Primary Hash, the switch will use the Secondary Hash.
Hash (MS Groups)	The hash function to use to decipher the encrypted Secret sent by the MS group member. Hash values are MD5 or SHA-1.
Primary Secret (ISL and Port Groups)	Hexadecimal string that is encrypted by the Primary Hash for authentication with the member. The string has the following lengths depending on the Primary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Secondary Hash (ISL and Port Groups)	Hash function to use to decipher the encrypted Secondary Secret sent by the group member. Hash values are MD5 or SHA-1. The Secondary Hash is used when the Primary Hash is not available on the group member. The Primary Hash and the Secondary Hash cannot be the same.
Secondary Secret (ISL and Port Groups)	Hex string that is encrypted by the Secondary Hash and sent for authentication. The string has the following lengths depending on the Secondary Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte

Table A-8. Group Member Attributes (Continued)

Attribute	Description
Secret (MS Groups)	Hexadecimal string that is encrypted by the Hash function for authentication with MS group members. The string has the following lengths depending on the Hash function: ■ MD5 hash: 16-byte ■ SHA-1 hash: 20-byte
Binding (ISL Groups)	Domain ID of the switch to which to bind the ISL group member worldwide name. This option is available only if FabricBindingEnabled is set to True using the Set Config Security command. Refer to the ”Set Config Command” on page A-61. 0 (zero) specifies no binding.

list
Displays a list of all groups and the security sets of which they are members. This keyword is available without an Admin session.

members [group]
Displays all members of the group given by [group]. This keyword is available without an Admin session.

remove [group] [member_list]
Remove the port/device worldwide name given by [member] from the group given by [group]. Use a <space> to delimit multiple member names in [member_list]

rename [group_old] [group_new]
Renames the group given by [group_old] to the group given by [group_new].

securitysets [group]
Displays the list of security sets of which the group given by [group] is a member. This keyword is available without an Admin session.

type [group]
Displays the group type for the group given by [group]. This keyword is available without an Admin session.

Notes

Refer to the ”Securityset Command” on page A-57 for information about managing groups in security sets.

Examples

The following is an example of the Group Add command:

```
SANbox Manager (admin-security) #> group add Group_1

  A list of attributes with formatting and default values will follow
  Enter a new value or simply press the ENTER key to accept the current value
  with exception of the Group Member WWN field which is mandatory.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Group Name       Group_1
  Group Type       ISL
  Member           (WWN)                            [00:00:00:00:00:00:00:00]
  Authentication   (None / Chap)                    [None                    ]
  PrimaryHash      (MD5 / SHA-1)                    [MD5                     ]
  PrimarySecret    (32 hex or 16 ASCII char value)  [                        ]
  SecondaryHash    (MD5 / SHA-1 / None)             [None                    ]
  SecondarySecret  (40 hex or 20 ASCII char value)  [                        ]
  Binding          (domain ID 1-239, 0=None)        [0                       ]


  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group Edit command:

```
SANbox Manager (admin-security) #> group edit G1 10:00:00:c0:dd:00:90:a3
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Group Name        g1
  Group Type        ISL
  Group Member      10:00:00:c0:dd:00:90:a3
  Authentication    (None / Chap)                    [None]  chap
  PrimaryHash       (MD5 / SHA-1)                    [MD5 ]  sha-1
  PrimarySecret     (40 hex or 20 ASCII char value)  [    ]  12345678901234567890
  SecondaryHash     (MD5 / SHA-1 / None)             [None]  md5
  SecondarySecret   (32 hex or 16 ASCII char value)  [    ]  1234567890123456
  Binding           (domain ID 1-239, 0=None)        [3   ]


  Finished configuring attributes.
  To discard this configuration use the security cancel command.
```

The following is an example of the Group List command:

```
SANbox Manager #> group list
  Group       SecuritySet
  -----       -----------
  group1 (ISL)
              alpha
  group2 (Port)
              alpha
```

The following is an example of the Group Members command:

```
SANbox Manager #> group members group1
  Current list of members for Group: group1
  ---------------------------------
  10:00:00:c0:dd:00:71:ed
  10:00:00:c0:dd:00:72:45
  10:00:00:c0:dd:00:90:ef
  10:00:00:c0:dd:00:b8:b7
```

Hardreset Command

Resets the switch and performs a power-on self test. This reset disrupts traffic, activates the pending firmware, and clears the alarm log. To save the alarm log before resetting, refer to the ”Set Log Command” on page A-75.

Authority Admin session

Syntax **hardreset**

Notes To reset the switch without a power-on self test, refer to the ”Reset Command” on page A-45.

To reset the switch without disrupting traffic, refer to the ”Hotreset Command” on page A-36.

Help Command

Displays a brief description of the specified command, its keywords, and usage.

Authority None

Syntax **help *[command] [keyword]***

Keywords ***[command]***
Displays a summary of the command given by [command] and its keywords. If you omit [command], the system displays all available commands.

[keyword]
Displays a summary of the keyword given by [keyword] belonging to the command given by [command]. If you omit [keyword], the system displays the available keywords for the specified command.

all
Displays a list of all available commands (including command variations).

Examples The following is an example of the Help Config command:

```
SANbox Manager #> help config
config CONFIG_OPTIONS
The config command operates on configurations.

  Usage: config   { activate | backup   | cancel   | copy     | delete   |
                    edit     | list     | restore  | save }
```

The following is an example of the Help Config Edit command:

```
SANbox Manager #> help config edit
config edit [CONFIG_NAME]
This command initiates a configuration session and places the current session
into config edit mode.
If CONFIG_NAME is given and it exists, it gets edited; otherwise, it gets
created.  If it is not given, the currently active configuration is edited.

Admin mode is required for this command.

  Usage: config edit [CONFIG_NAME]
```

History Command

Displays a numbered list of the previously entered commands from which you can re-execute selected commands.

Authority None

Syntax **history**

Notes Use the History command to provide context for the ! command:

- Enter ![command_string] to re-execute the most recent command that matches [command_string].
- Enter ![line number] to re-execute the corresponding command from the History display
- Enter ![partial command string] to re-execute a command that matches the command string.
- Enter !! to re-execute the most recent command.

Examples The following is an example of the History command:

```
SANbox Manager #> history
   1 show switch
   2 date
   3 help set
   4 history

SANbox Manager #> !3
help set

set SET_OPTIONS
There are many attributes that can be set.
Type help with one of the following to get more information:

  Usage: set   { alarm     | beacon    | config    | log       | pagebreak |
                 port      | setup     | switch }
```

Hotreset Command

Resets the switch for the purpose of activating the pending firmware without disrupting traffic. This command terminates all management sessions, saves all configuration information, and clears the event log. After the pending firmware is activated, the configuration is recovered. This process takes less than 80 seconds. To save the event log to a file before resetting, refer to the ”Set Log Command” on page A-75.

Authority Admin session

Syntax **hotreset**

Notes

- You can load and activate version 5.0.x firmware on an operating switch without disrupting data traffic or having to re-initialize attached devices under the following conditions:
  - The current firmware version is a 4.2.x version that precedes the upgrade version.
  - No changes are being made to switches in the fabric including powering up, powering down, disconnecting or connecting ISLs, and switch configuration changes.
  - No port in the fabric is in the diagnostic state.
  - No zoning changes are being made in the fabric.
  - No changes are being made to attached devices including powering up, powering down, disconnecting, connecting, and HBA configuration changes.
- Ports that are stable when the non-disruptive activation begins, then change states, will be reset. When the non-disruptive activation is complete, SANsurfer Switch Manager sessions reconnect automatically. However, Telnet sessions must be restarted manually.
- This command clears the event log and all counters.

Image Command

Manages and installs switch firmware.

Authority Admin session

Syntax **image**

cleanup
fetch [account_name] [ip_address] [file_source] [file_destination]
install
list
unpack [file]

Keywords **cleanup**

Removes all firmware image files from the switch. All firmware image files are removed automatically each time the switch is reset.

fetch [account_name] [ip_address] [file_source] [file_destination]

Retrieves image file given by [file_source] and stores it on the switch with the file name given by [file_destination]. The image file is retrieved from the FTP server with the IP address given by [ip_address] and an account name given by [account_name]. If an account name needs a password to access the FTP server, the system will prompt you for it.

install

Downloads firmware from a remote host to the switch, installs the firmware, then resets the switch (without a power-on self test) to activate the firmware. If possible, a non-disruptive activation is performed. The command prompts you for the following:

- IP address of the remote host
- An account name and password on the remote host
- Pathname for the firmware image file

list

Displays the list of image files that reside on the switch.

unpack [file]

Installs the firmware file given by [file]. After unpacking the file, a message appears confirming successful unpacking. The switch must be reset for the new firmware to take effect.

Notes

To provide consistent performance throughout the fabric, ensure that all switches are running the same version of firmware.

To install firmware when the management workstation has an FTP server, use the Image Install command or the "Firmware Install Command" on page A-23. To install firmware when the management workstation does not have an FTP server, do the following:

1. Move to the folder or directory on the workstation that contains the new firmware image file.
2. Establish communications with the switch using the File Transfer Protocol (FTP). Enter one of the following on the command line:

   ```
   >ftp xxx.xxx.xxx.xxx
   ```

   or

   ```
   >ftp switchname
   ```

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
3. Enter the following account name and password:

   ```
   user:images
   password: images
   ```
4. Activate binary mode and copy the firmware image file on the switch:

   ```
   ftp>bin
   ftp>put filename
   ```
5. Wait for the transfer to complete, then close the FTP session.

   ```
   xxxxx bytes sent in xx secs.
   ftp>quit
   ```
6. Establish communications with the switch using the CLI. Enter one of the following on the command line:

   ```
   telnet xxx.xxx.xxx.xxx
   ```

   or

   ```
   telnet switchname
   ```

   where *xxx.xxx.xxx.xxx* is the switch IP address, and *switchname* is the switch name associated with the IP address.
7. A Telnet window opens prompting you for a login. Enter an account name and password. The default account name and password are (admin, password).
8. Open an Admin session to acquire the necessary authority.

   ```
   SANbox Manager $>admin start
   ```

9. Display the list of firmware image files on the switch to confirm that the file was loaded.

```
SANbox Manager (admin) $>image list
```

10. Unpack the firmware image file to install the new firmware in flash memory.

```
SANbox Manager (admin) $>image unpack filename
```

11. Wait for the unpack to complete.

```
image unpack command result: Passed
```

12. A message will prompt you to reset the switch to activate the firmware. Resetting the switch is disruptive. Use the Hotreset command to attempt a non-disruptive activation.

```
SANbox Manager (admin) $>hotreset
```

Examples The following is an example of the Image Install command:

```
SANbox Manager (admin) #> image install
 Warning: Installing new firmware requires a switch reset.
 Continuing with this action will terminate all management sessions,
 including any Telnet sessions. When the firmware activation is complete,
 you may log in to the switch again.
 Do you want to continue? [y/n]: y
    Press 'q' and the ENTER key to abort this command.

  User Account    : johndoe
  IP Address      : 10.20.33.130

  About to install image.  Do you want to continue? [y/n] y

Connected to 10.20.33.130 (10.20.33.130).
220 localhost.localdomain FTP server (Version wu-2.6.1-18) ready.
331 Password required for johndoe.
Password: xxxxxxxxx
230 User johndoe logged in.
bin
200 Type set to I.
verbose
Verbose mode off.
  This may take several seconds...
  The switch will now reset.
Connection closed by foreign host.
```

Lip Command

Reinitializes the specified loop port.

Authority Admin session

Syntax **lip [port_number]**

Keywords **[port_number]**
The number of the port to be reinitialized. Ports are numbered beginning with 0.

Examples The following is an example of the Lip command:

```
SANbox Manager (admin) #> lip 2
```

Passwd Command

Changes a user account's password.

Authority Admin account name and an admin session to change another account's password; You can change you own password without an Admin session.

Syntax **passwd [account_name]**

Keywords **[account_name]**
The user account name. To change the password for an account name other than your own, you must open an admin session with the account name Admin. If you omit [account_name], you will be prompted to change the password for the current account name.

Examples The following is an example of the Passwd command:

```
SANbox Manager (admin) #> passwd user2

     Press 'q' and the ENTER key to abort this command.

  account OLD password               : ********
  account NEW password (8-20 chars)  : ********

  please confirm account NEW password: ********
  password has been changed.
```

Ping Command

Initiates an attempt to communicate with another switch over an Ethernet network and reports the result.

Authority None

Syntax **ping [ip_address]**

Keywords **[ip_address]**
The IP address of the switch to query. Broadcast IP addresses, such as 255.255.255.255, are not valid.

Examples The following is an example of a successful Ping command:

```
SANbox Manager #> ping 10.20.11.57
  Ping command issued. Waiting for response...
SANbox Manager #>
  Response successfully received from 10.20.11.57.
```

This following is an example of an unsuccessful Ping command:

```
SANbox Manager #> ping 10.20.10.100
  Ping command issued. Waiting for response...
  No response from 10.20.10.100. Unreachable.
```

Ps Command

Displays current system process information.

Authority None

Syntax **ps**

Examples The following is an example of the Ps command:

```
SANbox Manager #> ps


PID  PPID %CPU     TIME     ELAPSED COMMAND
338   327  0.0 00:00:00  3-01:18:35 cns
339   327  0.0 00:00:01  3-01:18:35 ens
340   327  0.0 00:00:21  3-01:18:35 dlog
341   327  0.1 00:05:35  3-01:18:35 ds
342   327  0.2 00:11:29  3-01:18:35 mgmtApp
343   327  0.0 00:00:04  3-01:18:35 fc2
344   327  0.0 00:02:16  3-01:18:35 nserver
345   327  0.0 00:02:44  3-01:18:35 mserver
346   327  0.8 00:35:12  3-01:18:35 util
347   327  0.0 00:00:29  3-01:18:35 snmpservicepath
348   327  0.0 00:02:46  3-01:18:34 eport
349   327  0.0 00:00:21  3-01:18:34 PortApp
350   327  5.6 04:08:24  3-01:18:34 port_mon
351   327  0.0 00:01:38  3-01:18:34 zoning
352   327  0.0 00:00:01  3-01:18:34 diagApp
404   327  0.0 00:00:04  3-01:18:27 snmpd
405   327  0.0 00:00:02  3-01:18:27 snmpmain
406   405  0.0 00:00:00  3-01:18:26 snmpmain
```

Quit Command

Closes the Telnet session.

Authority None

Syntax **quit, exit, or logout**

Notes You can also enter Control-D to close the Telnet session.

Reset Command

Resets the switch configuration parameters. If you omit the keyword, the default is Reset Switch.

Authority Admin session

Syntax **reset**

config *[config_name]*
factory
port [port_number]
radius
security
services
snmp
switch (default)
system
zoning

Keywords **config *[config_name]***

Resets the configuration given by [config_name] to the factory default values for switch, port, port threshold alarm, and zoning configuration as described in Table A-9 through Table A-12. If [config_name] does not exist on the switch, a configuration with that name will be created. If you omit [config_name], the active configuration is reset. You must activate the configuration for the changes to take effect. for switch, port, and port threshold alarm configuration default values.

factory

Resets switch configuration, port configuration, port threshold alarm configuration, zoning configuration, SNMP configuration, system configuration, security configuration, RADIUS configuration, switch services configuration, and zoning to the factory default values as described in Table A-9 through Table A-17. The switch configuration is activated automatically.

Note:

- Because this keyword changes network parameters, the workstation could lose communication with the switch and release the Admin session.
- This keyword does not affect installed license keys.

port [port_number]

Reinitializes the port given by [port_number]. Ports are numbered beginning with 0.

radius

Resets the RADIUS configuration to the default values as described in Table A-14.

security
Clears the security database and deactivates the active security set. The security configuration value, autosave, and fabric binding remain unchanged.

services
Resets the switch services configuration to the default values as described in Table A-15.

snmp
Resets the SNMP configuration settings to the factory default values. Refer to Table A-13 for SNMP configuration default values.

switch
Resets the switch without a power-on self test. This is the default. This reset disrupts traffic and does the following:

- Activates the pending firmware.
- Closes all management sessions.
- Clears the event log. To save the event log before resetting, refer to the ”Set Log Command” on page A-75.

To reset the switch with a power-on self test, refer to the ”Hardreset Command” on page A-33. To reset the switch without disrupting traffic, refer to the ”Hotreset Command” on page A-36.

system
Resets the system configuration settings to the factory default values. as described in Table A-16.

Note:
- Because this keyword changes network parameters, the workstation could lose communication with the switch.
- This keyword does not affect installed license keys.

zoning
Clears the zoning database and deactivates the active zone set. The zoning configuration values (autosave, default visibility) remain unchanged.

Notes

The following tables specify the various factory default settings:

Enter the Show Config Switch command to display switch configuration values.

Table A-9. Switch Configuration Defaults

Parameter	Default
Admin State	Online
Broadcast Enabled	True
InbandEnabled	True
FDMIEnabled	True
FDMIEntries	1000
DefaultDomain ID	1 (0x Hex)
Domain ID Lock	False
Symbolic Name	SANbox Manager
R_A_TOV	10000
E_D_TOV	2000
Principal Priority	254
Configuration Description	Config Default
InteropMode	Standard
LegacyAddressFormat	False

Enter the Show Config Port command to display port configuration values.

Table A-10. Port Configuration Defaults

Parameter	1-Gbps/2-Gbps Port Defaults	10-Gbps Port Defaults
Admin State	Online	Online
Link Speed	Auto	10-Gbps
Port Type	GL	G
Symbolic Name	Portn, where n is the port number	10G-n, where n is the port number
ALFairness	False	N/A
DeviceScanEnabled	True	True
ForceOfflineRSCN	False	False
ARB_FF	False	N/A
InteropCredit	0	0
ExtCredit	0	N/A
FANEnable	True	N/A
AutoPerfTuning	True	True
LCFEnable	False	False
MFSEnable	False	False
MSEnable	True	False
NoClose	False	N/A
IOStreamGuard	Auto	Auto
VIEnable	False	False
PDISCPingEnable	True	N/A

Enter Show Config Threshold command to display threshold alarm configuration values.

Table A-11. Port Threshold Alarm Configuration Defaults

Parameter	Default
ThresholdMonitoringEnabled	False
CRCErrorsMonitoringEnabled	True
RisingTrigger	25
FallingTrigger	1
SampleWindow	10
DecodeErrorsMonitoringEnabled	True
RisingTrigger	200
FallingTrigger	0
SampleWindow	10
ISLMonitoringEnabled	True
RisingTrigger	2
FallingTrigger	0
SampleWindow	10
LoginMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LogoutMonitoringEnabled	True
RisingTrigger	5
FallingTrigger	1
SampleWindow	10
LOSMonitoringEnabled	True
RisingTrigger	100
FallingTrigger	5
SampleWindow	10

Enter the Show Config Zoning command to display zoning configuration values.

Table A-12. Zoning Configuration Defaults

Parameter	Default
InteropAutoSave	True
DefaultVisibility	All
DiscardInactive	False

Enter the Show Setup SNMP command to display SNMP configuration values.

Table A-13. SNMP Configuration Defaults

Parameter	Default
SNMPEnabled	True
Contact	<syscontact undefined>
Location	<sysLocation undefined>
Description	SANbox 5602 FC Switch
Trap [1-5] Address	Trap 1: 10.0.0.254; Traps 2–5: 0.0.0.0
Trap [1-5] Port	162
Trap [1-5] Severity	Warning
Trap [1-5] Version	2
Trap [1-5] Enabled	False
ObjectID	1.3.6.1.4.1.1663.1.1.1.1.24
AuthFailureTrap	False
ProxyEnabled	True

Enter the Show Setup Radius command to display RADIUS configuration values.

Table A-14. RADIUS Configuration Defaults

Parameter	Default
DeviceAuthOrder	Local
UserAuthOrder	Local
TotalServers	1
DeviceAuthServer	False
UserAuthServer	False
AccountingServer	False
ServerIPAddress	10.0.0.1
ServerUDPPort	1812
Timeout	2 seconds

Table A-14. RADIUS Configuration Defaults (Continued)

Parameter	Default
Retries	0
SignPackets	False

Enter the Show Setup Services command to display switch service configuration values.

Table A-15. Services Configuration Defaults

Parameter	Default
TelnetEnabled	True
SSHEnabled	False
GUIMgmtEnabled	True
SSLMgmtEnabled	False
EmbeddedGUIEnabled	True
SNMPEnabled	True
NTPEnabled	False
CIMEnabled	True
FTPEnabled	True.
MgmtServerEnabled	False

Enter the Show Setup System command to display system configuration values.

Table A-16. System Configuration Defaults

Parameter	Default
Ethernet Network Discovery	Static
Ethernet Network IP Address	10.0.0.1
Ethernet Network IP Mask	255.0.0.0
Ethernet Gateway Address	10.0.0.254
Admin Timeout	30 minutes
InactivityTimeout	0
LocalLogEnabled	True
RemotelogEnabled	False
RemoteLogHostAddress	10.0.0.254
NTPClientEnabled	False
NTPServerAddress	10.0.0.254
EmbeddedGUIEnabled	True

Enter the Show Config Security command to display security configuration values.

Table A-17. Security Configuration Defaults

Parameter	Default
AutoSave	True
FabricBindingEnabled	True

Security Command

Opens a Security Edit session in which to manage the security database on a switch. Refer to the ”Group Command” on page A-25 and the ”Securityset Command” on page A-57.

Authority Admin session. The keywords Active, History, Limits, and List are available without an Admin session.

Syntax

security
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays the active security set, its groups, and group members. This keyword does not require an Admin session.

cancel
Closes a Security Edit session without saving changes. Use the Edit keyword to open a Security Edit session.

clear
Clears all inactive security sets from the volatile edit copy of the security database. This keyword does not affect the non-volatile security database. However, if you enter the Security Clear command followed by the Security Save command, the non-volatile security database will be cleared from the switch.

Note: The preferred method for clearing the security database from the switch is the Reset Security command. Refer to the ”Reset Command” on page A-45.

edit
Initiates a Security Edit session in which to make changes to the security database. A Security Edit session enables you to use the Group and Securityset commands to create, add, and delete security sets, groups, and group members. To close a Security Edit session and save changes, enter the Security Save command. To close a Security Edit session without saving changes, enter the Security Cancel command.

history
Displays history information about the security database and the active security set including the account name that made changes and when those changes were made. This keyword does not require an Admin session.

limits
Displays the current totals and the security database limits for the number of security sets, groups, members per group, and total members. This keyword does not require an Admin session.

list
Displays all security sets, groups, and group members in the security database. This keyword does not require an Admin session.

restore
Reverts the changes to the security database that have been made during the current Security Edit session since the last Security Save command was entered.

save
Saves the changes that have been made to the security database during a Security Edit session. Changes you make to any security set will not take effect until you activate that security set. Refer to the ”Securityset Command” on page A-57 for information about activating a security set.

Examples

The following is an example of the Security Active command:

```
SANbox Manager #> security active
  Active Security Information

  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

The following is an example of the Security History command:

```
SB211.192 #> security history
  Active Database Information
  ---------------------------
  SecuritySetLastActivated/DeactivatedBy  Remote
  SecuritySetLastActivated/DeactivatedOn  day month date time year
  Database Checksum                   00000000

  Inactive Database Information
  -----------------------------
  ConfigurationLastEditedBy           admin@IB-session11
  ConfigurationLastEditedOn           day month date time year
  Database Checksum                   00007558
```

The following is an example of the Security Limits command:

```
SANbox Manager #> security limits
  Security Attribute   Maximum   Current   [Name]
  ------------------   -------   -------   ------
  MaxSecuritySets      4         1
  MaxGroups            16        2
  MaxTotalMembers      1000      19
  MaxMembersPerGroup   1000
                                 4         group1
                                 15        group2
```

The following is an example of the Security List command:

```
SANbox Manager (admin-security) #> security list
SB211.192 #> security list
  Active Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  No active securityset defined.

  Configured Security Information
  SecuritySet  Group  GroupMember
  -----------  -----  -----------
  alpha
               group1 (ISL)
                      10:00:00:00:00:10:21:16
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
                      10:00:00:00:00:10:21:17
                         Authentication     Chap
                         Primary Hash       MD5
                         Primary Secret     ********
                         Secondary Hash     SHA-1
                         Secondary Secret   ********
                         Binding            0
```

Securityset Command

Manages security sets in the security database.

Authority Admin session and a Security Edit session. Refer to the "Security Command" on page A-53 for information about starting a Security Edit session. The Active, Groups, and List keywords are available without an Admin session. You must close the Security Edit session before using the Activate and Deactivate keywords.

Syntax

securityset
activate [security_set]
active
add [security_set] [group_list]
copy [security_set_source] [security_set_destination]
create [security_set]
deactivate
delete [security_set]
groups [security_set]
list
remove [security_set] [group]
rename [security_set_old] [security_set_new]

Keywords

activate [security_set]
Activates the security set given by [security_set]. This keyword deactivates the active security set. Close the Security Edit session using the Security Save or Security Cancel command before using this keyword.

active
Displays the name of the active security set. This keyword is available to without an Admin session.

add [security_set] [group_list]
Adds one or more groups given by [group_list] to the security set given by [security_set]. Use a <space> to delimit multiple group names in [group_list]. A security set can have a maximum of three groups with no more than one group of each group type.

copy [security_set_source] [security_set_destination]
Creates a new security set named [security_set_destination] and copies into it the membership from the security set given by [security_set_source].

create [security_set]
Creates the security set with the name given by [security_set]. A security set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The security database supports a maximum of 4 security sets.

deactivate
Deactivates the active security set. Close the Security Edit session before using this keyword.

delete [security_set]
Deletes the security set given by [security_set]. If the specified security set is active, the command is suspended until the security set is deactivated.

groups [security_set]
Displays all groups that are members of the security set given by [security_set]. This keyword is available without an Admin session.

list
Displays a list of all security sets. This keyword is available without an Admin session.

remove [security_set] [group]
Removes a group given by [group] from the security set given by [security_set]. If [security_set] is the active security set, the group will not be removed until the security set has been deactivated.

rename [security_set_old] [security_set_new]
Renames the security set given by [security_set_old] to the name given by [security_set_new].

Notes

Refer to the ”Group Command” on page A-25 for information about creating and managing groups.

Examples

The following is an example of the Securityset Active command

```
SANbox Manager #> securityset active
  Active SecuritySet Information
  ------------------------------
  ActiveSecuritySet alpha
  LastActivatedBy  Remote
  LastActivatedOn  day month date time year
```

The following is an example of the Securityset Groups command

```
SANbox Manager #> securityset groups alpha
  Current list of Groups for SecuritySet: alpha
  --------------------------------------
  group1 (ISL)
  group2 (Port)
```

The following is an example of the Securityset List command

```
SANbox Manager #> securityset list
Current list of SecuritySets
----------------------------
  alpha
  beta
```

Set Command

Sets a variety of switch parameters.

Authority Admin session for all keywords except Alarm, Beacon, and Pagebreak which are available without an Admin session.

Syntax

set
alarm [option]
beacon [state]
config [option]
log [option]
pagebreak [state]
port [option]
setup [option]
switch [state]
timezone

Keywords

alarm [option]
Controls the display of alarms in the session output stream or clears the alarm log. [option] can be one of the following:

clear
Clears the alarm log history. This value requires an Admin session.

on
Enables the display of alarms in the session output stream.

off
Disables the display of alarms in the session output stream.

beacon [state]
Enables or disables the flashing of the Logged-In LEDs according to [state]. This keyword does not require an admin session. [state] can be one of the following:

on
Enables the flashing beacon.

off
Disables the flashing beacon.

config [option]
Sets switch, port, port threshold alarm, security, and zoning configuration parameters. Refer to the ”Set Config Command” on page A-61.

log [option]
Specifies the type of entries to be entered in the event log. Refer to the ”Set Log Command” on page A-75.

pagebreak [state]
Specifies how much information is displayed on the screen at a time according to the value given by [state]. This keyword does not require an admin session. [state] can be one of the following:

on
Limits the display of information to 20 lines at a time. The page break functions affects the following commands: Alias (List, Members), Show (Alarm, Log), Zone (List, Members), Zoneset (List, Zones), Zoning (Active, List).

off
Allows continuous display of information without a break.

port [option]
Sets port state and speed for the specified port. The previous Set Config Port settings are restored after a switch reset or a reactivation of a switch configuration. Refer to the ”Set Port Command” on page A-79.

setup [option]
Changes SNMP and system configuration settings. Refer to the ”Set Setup Command” on page A-81.

switch [state]
Changes the administrative state for all ports on the switch to the state given by [state]. The previous Set Config Switch settings are restored after a switch reset or a reactivation of a switch configuration. [state] can be one of the following:

online
Places all ports online

offline
Places all ports offline.

diagnostics
Prepares all ports for testing.

timezone
Specifies the time zone for the switch and the workstation. The default is Universal Time (UTC) also known as Greenwich Mean Time (GMT). This keyword prompts you to choose a region, then a subregion to specify the time zone.

Examples

The following examples enables and disables the beacon:

```
SANbox Manager #> set beacon on

  Command succeeded.

SANbox Manager $> set beacon off

  Command succeeded.
```

Set Config Command

Sets switch, port, port threshold alarm, security, and zoning configuration parameters. The changes you make with this command are not retained when you reset or power cycle the switch unless you save them using the Config Save command. Refer to the ”Config Command” on page A-16.

Authority Admin session and a Config Edit session

Syntax

set config
port *[port_number]*
ports *[port_number]*
security
switch
threshold
zoning

Keywords

port *[port_number]*
Initiates an edit session in which to change configuration parameters for the port number given by [port_number]. If you omit [port_number], the system begins with port 0 and proceeds in order through the last port. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration for one port, or “qq” to end the configuration for all ports. Table A-18 describes the port parameters.

ports *[port_number]*
Initiates an editing session in which to change configuration parameters for all ports based on the configuration for the port given by [port_number]. If you omit [port_number], port 0 is used. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” to end the configuration. Table A-18 describes the port parameters.

Table A-18. Set Config Port Parameters

Parameter	Description
AdminState	Port administrative state: ■ Online – Activates and prepares the port to send data. This is the default. ■ Offline – Prevents the port from receiving signal and accepting a device login. ■ Diagnostics – Prepares the port for testing and prevents the port from accepting a device login. ■ Down – Disables the port by removing power from the port lasers.
LinkSpeed	Transmission speed: ■ 1-Gbps/2-Gbps Ports: 1-Gbps, 2 Gbps, 4-Gbps, or Auto. The default is Auto. ■ 10-Gbps Ports: 10-Gbps

Table A-18. Set Config Port Parameters (Continued)

Parameter	Description
PortType	Port type: ■ 1-Gbps/2-Gbps Ports: GL, G, F, FL, Donor. The default is GL. ■ 10-Gbps Ports: G
SymbolicPortName	Descriptive name for the port. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Port n where n is the port number.
ALFairness (1-Gbps/2-Gbps ports only)	Arbitration loop fairness. Enables (True) or disables (False) the switch's priority to arbitrate on the loop. The default is False.
DeviceScanEnabled	Enables (True) or disables (False) the scanning of the connected device for FC-4 descriptor information during login. The default is True.
ForceOfflineRSCN	Enables (False) or disables (True) the immediate transmission of RSCN messages when communication between a port and a device is interrupted. If enabled, the RSCN message is delayed for 200 ms for locally attached devices and 400 ms for devices connected through other switches. The default is False. This parameter is ignored if IOStreamGuard is enabled.
ARB_FF (1-Gbps/2-Gbps ports only)	Send ARB_FF (True) instead of IDLEs (False) on the loop. The default is False.
InteropCredit	Interoperability credit. The number of buffer-to-buffer credits per port. 0 means the default (16) is unchanged. Changing interoperability credits is necessary only for E_Ports that are connected to non-FC-SW-2-compliant switches. Contact your authorized maintenance provider for assistance in using this feature.
ExtCredit (1-Gbps/2-Gbps ports only)	Extended credits. The number of port buffer credits that this port can acquire from donor ports. The default is 0.
FANEnable (1-Gbps/2-Gbps ports only)	Fabric address notification. Enables (True) or disables (False) the communication of the FL_Port address, port name, and node name to the logged-in NL_Port. The default is True.

Table A-18. Set Config Port Parameters (Continued)

Parameter	Description
AutoPerfTuning	Automatic performance tuning for FL_Ports only. The default is True. ■ If AutoPerfTuning is enabled (True) and the port is an FL_Port, MFSEnable is automatically enabled. LCFEnable and VIEnable are overridden to False. ■ If AutoPerfTuning is disabled (False), MFSEnable, LCFEnable, and VIEnable retain their original values.
LCFEnable	Link control frame preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) preferred routing of frames with R_CTL = 1100 (Class 2 responses). The default is False. Enabling LCFEnable will disable MFSEnable.
MFSEnable	Multi-Frame Sequence bundling. This parameter appears only if AutoPerfTuning is False. Prevents (True) or allows (False) the interleaving of frames in a sequence. The default is False. Enabling MFSEnable disables LCFEnable and VIEnable.
VIEnable	Virtual Interface (VI) preference routing. This parameter appears only if AutoPerfTuning is False. Enables (True) or disables (False) VI preference routing. The default is False. Enabling VIEnable will disable MFSEnable.
MSEnable	Management server enable. Enables (True) or disables (False) management server on this port. The default is True.
NoClose (1-Gbps/2-Gbps ports only)	Loop circuit closure prevention. Enables (True) or disables (False) the loop's ability to remain in the open state indefinitely. True reduces the amount of arbitration on a loop when there is only one device on the loop. The default is False.

Table A-18. Set Config Port Parameters (Continued)

Parameter	Description
IOStreamGuard	I/O Stream Guard. Enables or disables the suppression of RSCN messages. IOStreamGuard can have the following values: ■ Enable – Suppresses the reception of RSCN messages from other ports for which IOStreamGuard is enabled. ■ Disable – Allows free transmission and reception of RSCN messages. ■ Auto – Suppresses the reception of RSCN messages when the port is connected to an initiator device with a QLogic HBA. For older QLogic HBAs, such as the QLA2200, the DeviceScanEnabled parameter must also be enabled. The default is Auto.
PDISCPingEnable (1-Gbps/2-Gbps ports only)	Enables (True) or disables (False) the transmission of ping messages from the switch to all devices on a loop port. The default is True.

security
Initiates an editing session in which to change the security settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Enter “q” or "Q" to end the editing session. Table A-19 describes the Set Config Security parameters.

Table A-19. Security Configuration Parameters

Parameter	Description
AutoSave	Enables (True) or disables (False) the saving of changes to active security set in the switch’s permanent memory. The default is True.
FabricBindingEnabled	Enables (True) or disables (False) the configuration and enforcement of fabric binding on all switches the fabric. Fabric binding associates switch worldwide names with a domain ID in the creation of ISL groups.

switch
Initiates an editing session in which to change switch configuration settings. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. Table A-20 describes the Set Config Switch parameters.

Table A-20. Set Config Switch Parameters

Parameter	Description
AdminState	Switch administrative state: online, offline, or diagnostics. The default is Online.
BroadcastEnabled	Broadcast. Enables (True) or disables (False) forwarding of broadcast frames. The default is True.
InbandEnabled	Inband management. Enables (True) or disables (False) the ability to manage the switch over an ISL. The default is True.
FDMIEnabled	Fabric Device Monitoring Interface. Enables (True) or disables (False) the monitoring of target and initiator device information. The default is True.
FDMIEntries	The number of device entries to maintain in the FDMI database. Enter a number from 0–1000. The default is 1000.
DefaultDomainID	Default domain ID. The default is 1.
DomainIDLock	Prevents (True) or allows (False) dynamic reassignment of the domain ID. The default is False.
SymbolicName	Descriptive name for the switch. The name can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is SANbox Manager.
R_A_TOV	Resource Allocation Timeout Value. The number of milliseconds the switch waits to allow two ports to allocate enough resources to establish a link. The default is 10000.
E_D_TOV	Error Detect Timeout Value. The number of milliseconds a port is to wait for errors to clear. The default is 2000.
PrincipalPriority	The priority used in the FC-SW-2 principal switch selection algorithm. 1 is high, 255 is low. The default is 254.
ConfigDescription	Switch configuration description. The configuration description can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is Config Default.

Table A-20. Set Config Switch Parameters (Continued)

Parameter	Description
InteropMode	Propagates just the active zone set throughout the fabric (Standard, FC-SW-2 compliant) or the entire zoning database (Interop-1, non-compliant). The default is Standard.
LegacyAddressFormat	Available only when the InteropMode parameter is Interop-1, this parameter enables (True) or disables (False) the use of legacy address formatting for interoperating with non-FC-SW-2 switches. The default is False.

threshold
Initiates a configuration session by which to generate and log alarms for selected events. The system displays each event, its triggers, and sampling window one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets. These parameters must be saved in a configuration and activated before they will take effect. Refer to the ”Config Command” on page A-16 for information about saving and activating a configuration. Table A-21 describes the Set Config Threshold parameters. The switch will down a port if an alarm condition is not cleared within three consecutive sampling windows (by default 30 seconds). Reset the port to bring it back online. An alarm is cleared when the threshold monitoring detects that the error rate has fallen below the falling trigger.

Table A-21. Set Config Threshold Parameters

Parameter	Description
Threshold Monitoring Enabled	Master enable/disable parameter for all events. Enables (True) or disables (False) the generation of all enabled event alarms. The default is False.
CRCErrorsMonitoringEnabled DecodeErrorsMonitoringEnabled ISLMonitoringEnabled LoginMonitoringEnabled LogoutMonitoringEnabled LOSMonitoringEnabled	The event type enable/disable parameter. Enables (True) or disables (False) the generation of alarms for each of the following events: ■ CRC errors ■ Decode errors ■ ISL connection count ■ Device login errors ■ Device logout errors ■ Loss-of-signal errors
Rising Trigger	The event count above which a rising trigger alarm is logged. The switch will not generate another rising trigger alarm for that event until the count descends below the falling trigger and again exceeds the rising trigger.
Falling Trigger	The event count below which a falling trigger alarm is logged. The switch will not generate another falling trigger alarm for that event until the count exceeds the rising trigger and descends again below the falling trigger.
Sample Window	The period of time in seconds in which to count events.

zoning
Initiates an editing session in which to change switch zoning attributes. The system displays each parameter one line at a time and prompts you for a value. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table A-22. Set Config Zoning Parameters

Parameter	Description
InteropAutoSave	Available only when the InteropMode parameter is Standard, this parameter enables (True) or disables (False) the saving of changes to active zone set in the switch's permanent memory. Refer to "InteropMode" on page A-66. The default is True. Disabling the Autosave parameter can be useful to prevent the propagation of zoning information when experimenting with different zoning schemes. However, leaving the Autosave parameter disabled can disrupt device configurations should a switch have to be reset. For this reason, the Autosave parameter should be enabled in a production environment.
DefaultVisibility	Enables (All) or disables (None) communication among the switch's ports/devices and the fabric in the absence of an active zone set. The default is All.
DiscardInactive	Enables (True) or disables (False) the discarding of all inactive zone sets from that zoning database. Inactive zone sets are all zone sets except the active zone set. The default is False.

Examples

The following is an example of the Set Config Port command:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config edit
SANbox Manager (admin-config) #> set config port 1

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  1
  ------------------------

  AdminState    (1=Online, 2=Offline, 3=Diagnostics, 4=Down)       [Online]
  LinkSpeed     (1=1Gb/s, 2=2Gb/s, 3=Auto)                         [Auto  ]
  PortType      (GL / G / F / FL / Donor)                          [GL    ]
  SymPortName   (string, max=32 chars)                             [Port1 ]
  ALFairness    (True / False)                                     [False ]
  DeviceScanEnable (True / False)                                  [True  ]
  ForceOfflineRSCN (True / False)                                  [False ]
  ARB_FF        (True / False)                                     [False ]
  InteropCredit (decimal value, 0-255)                             [0     ]
  FANEnable     (True / False)                                     [True  ]

  AutoPerfTuning (True / False)                                    [False ]
  LCFEnable     (True / False)                                     [False ]
  MFSEnable     (True / False)                                     [False ]
  VIEnable      (True / False)                                     [False ]
  MSEnable      (True / False)                                     [True  ]
  NoClose       (True / False)                                     [False ]
  IOStreamGuard (Enable / Disable / Auto)                          [Disable]
  PDISCPingEnable  (True / False)                                  [True  ]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
SANbox Manager (admin-config) #>
```

The following is an example of the Set Config Port command for a 10-Gbps port:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config edit
SANbox Manager (admin-config) #> set config port 16

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  Configuring Port Number:  16
  ------------------------

AdminState       (1=Online, 2=Offline, 3=Diagnostics, 4=Down) [Online  ]
LinkSpeed        (10=10Gb/s)                                  [10Gb/s  ]
PortType         (G / F)                                      [G       ]
SymPortName      (string, max=32 chars)                       [10G-16  ]
DeviceScanEnable (True / False)                               [True    ]
ForceOfflineRSCN (True / False)                               [False   ]
AutoPerfTuning   (True / False)                               [Fales   ]
LCFEnable        (True / False)                               [False   ]
MFSEnable        (True / False)                               [False   ]
VIEnable         (True / False)                               [False   ]
MSEnable         (True / False)                               [True    ]
IOStreamGuard    (Enable / Disable / Auto)                    [Disabled]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
SANbox Manager (admin-config) #>
```

The following is an example of the Set Config Security command:

```
SANbox Manager #> admin start

SANbox Manager (admin) #> config edit

SANbox Manager (admin-config) #> set config security

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.


  FabricBindingEnabled  (True / False)     [False]
  AutoSave              (True / False)     [True ]


  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Switch command:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config edit
SANbox Manager (admin-config) #> set config switch

  A list of attributes with formatting and default values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

  AdminState          (1=Online, 2=Offline, 3=Diagnostics)   [Online        ]
  BroadcastEnabled    (True / False)                         [True          ]
  InbandEnabled       (True / False)                         [True          ]
  FDMIEnabled        (True / False)                          [True         ]
  FDMIEntries        (decimal value, 0-1000)                 [1000         ]
  DefaultDomainID     (decimal value, 1-239)                 [2             ]
  DomainIDLock        (True / False)                         [False         ]
  SymbolicName        (string, max=32 chars)                 [SANbox        ]
  R_A_TOV             (decimal value, 100-100000 msec)       [10000         ]
  E_D_TOV             (decimal value, 10-20000 msec)         [2000          ]
  PrincipalPriority   (decimal value, 1-255)                 [254           ]
  ConfigDescription   (string, max=64 chars)                 [Default Config]
  InteropMode         (0=Standard, 1=Interop_1)              [Standard      ]
```

The following is an example of the Set Config Threshold command:

```
SANbox Manager #> admin start
SANbox Manager  (admin) #> config edit
SANbox Manager (admin-config) #> set config threshold
A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.
ThresholdMonitoringEnabled     (True / False)              [False     ]

CRCErrorsMonitoringEnabled     (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [25        ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

DecodeErrorsMonitoringEnabled  (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [200       ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

ISLMonitoringEnabled           (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [2         ]
  FallingTrigger               (decimal value, 0-1000)     [0         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

LoginMonitoringEnabled         (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

LogoutMonitoringEnabled        (True / False)              [True      ]
  RisingTrigger                (decimal value, 1-1000)     [5         ]
  FallingTrigger               (decimal value, 0-1000)     [1         ]
  SampleWindow                 (decimal value, 1-1000 sec) [10        ]

LOSMonitoringEnabled           (True / False)               [True     ]
  RisingTrigger                (decimal value, 1-1000)     [100      ]
  FallingTrigger               (decimal value, 0-1000)     [5        ]
  SampleWindow                 (decimal value, 1-1000 sec) [10       ]
Finished configuring attributes.
This configuration must be saved (see config save command) and
activated (see config activate command) before it can take effect.
To discard this configuration use the config cancel command.
```

The following is an example of the Set Config Zoning command.

```
SANbox Manager #> admin start
SANbox Manager (admin) #> config edit
SANbox Manager (admin-config) #> set config zoning

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list press 'q'
or 'Q' and the ENTER key to do so.

  InteropAutoSave      (True / False)  [True]
  DefaultVisibility    (All / None)    [All ]
  DiscardInactive      (True / False)  [False]

  Finished configuring attributes.
  This configuration must be saved (see config save command) and
  activated (see config activate command) before it can take effect.
  To discard this configuration use the config cancel command.
```

Set Log Command

Specifies the events to record in the event log and display on the screen. You determine what events to record in the switch event log using the Component, Level, and Port keywords. You determine what events are automatically displayed on the screen using the Display keyword. Alarms are always displayed on the screen.

Authority Admin session

Syntax

set log
archive
clear
component [filter_list]
display [filter]
level [filter]
port [port_list]
restore
save
start (default)
stop

Keywords

archive
Collects all log entries and stores the result in new file named *logfile* that is maintained in switch memory where it can be downloaded using FTP. To download *logfile*, open an FTP session, log in with account name/password of “images” for both, and type “get logfile”.

clear
Clears all log entries.

component [filter_list]
Specifies one or more components given by [filter_list] to monitor for events. A component is a firmware module that is responsible for a particular portion of switch operation. Use a <space> to delimit values in the list. [filter_list] can be one or more of the following:

All
Monitors all components. To maintain optimal switch performance, do not use this setting with the Level keyword set to Info.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events.

SNMP
Monitors all SNMP events.

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

display [filter]
Specifies the log events to automatically display on the screen according to the event severity levels given by [filter]. [filter] can be one of the following values:

Critical
Critical severity level events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn
Warning severity level events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info
Informative severity level events. The informative level describes routine events associated with a normal fabric.

None
Specifies no severity levels for display on the screen.

level [filter]
Specifies the severity level given by [filter] to use in monitoring and logging events for the specified components or ports. [filter] can be one of the following values:

Critical
Monitors critical events. The critical level describes events that are generally disruptive to the administration or operation of the fabric, but require no action.

Warn
Monitors warning and critical events. The warning level describes events that are generally not disruptive to the administration or operation of the fabric, but are more important than the informative level events.

Info
Monitors informative, warning, and critical events. The informative level describes routine events associated with a normal fabric. This is the default severity level.

None
Monitors none of the severity levels.

port [port_list]
Specifies one or more ports to monitor for events. Choose one of the following values:

[port_list]
Specifies port or ports to monitor. Use a <space> to delimit values in the list. Ports are numbered beginning with 0.

All
Specifies all ports.

None
Disables monitoring on all ports.

restore
Restores and saves the port, component, and level settings to the default values.

save
Saves the log settings for the component, severity level, port, and display level. These settings remain in effect after a switch reset. The log settings can be viewed using the Show Log Settings command. To export log entries to a file, use the Set Log Archive command.

start
Starts the logging of events based on the Port, Component, and Level keywords assigned to the current configuration. The logging continues until you enter the Set Log Stop command.

stop
Stops logging of events.

Notes In addition to critical, warn, and informative severity levels, the highest event severity level is alarm. The alarm level describes events that are disruptive to the administration or operation of a fabric and require administrator intervention. Alarms are always logged and always displayed on the screen.

Set Port Command

Sets port state and speed for the specified port temporarily until the next switch reset or new configuration activation. This command also clears port counters.

Authority Admin session except for the Clear keyword.

Syntax

set port [port_number]
bypass [alpa]
clear
enable
speed [transmission_speed]
state [state]

Keywords

[port_number]
Specifies the port. Ports are numbered beginning with 0.

bypass [alpa]
Sends a Loop Port Bypass (LPB) to a specific Arbitrated Loop Physical Address (ALPA) or to all ALPAs on the arbitrated loop. [alpa] can be a specific ALPA or the keyword ALL to choose all ALPAs.

clear
Clears the counters on the port. This keyword does not require an admin session.

enable
Sends a Loop Port Enable (LPE) to all ALPAs on the arbitrated loop.

speed [transmission_speed]
Specifies the transmission speed for the specified port. Choose one of the following port speed values:

1Gb/s
One gigabit per second. This applies only to ports 0–15.

2Gb/s
Two gigabits per second. This applies only to ports 0–15.

4Gb/s
Four gigabits per second. This applies only to ports 0–15.

10Gb/s
Ten gigabits per second. This applies only to ports 16–19.

Auto
The port speed is automatically detected. This applies only to ports 0–15.

state [state]
Specifies one of the following administrative states for the specified port:

Online
Places the port online. This activates and prepares the port to send data.

Offline
Places the port offline. This prevents the port from receiving signal and accepting a device login.

Diagnostics
Prepares the port for testing. This prepares the port for testing and prevents the port from accepting a device login.

Down
Disables the port by removing power from the port lasers.

Set Setup Command

Manages configuration settings for Remote Authentication Dial-In User Service (RADIUS) servers, switch services, SNMP, and system configurations.

Authority Admin session

Syntax **set setup**
radius
services
snmp
system

Keywords **radius**
Prompts you in a line-by-line fashion to configure RADIUS servers for user account and device authentication. Table A-23 describes the RADIUS server configuration fields.

Table A-23. RADIUS Service Settings

Entry	Description
DeviceAuthOrder	Authenticator priority for devices: ■ Local: Authenticate devices using only the local security database. This is the default. ■ Radius: Authenticate devices using only the security database on the RADIUS server. ■ RadiusLocal: Authenticate devices using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
UserAuthOrder	Authenticator priority for user accounts: ■ Local: Authenticate users using only the local security database. This is the default. ■ Radius: Authenticate users using only the security database on the RADIUS server. ■ RadiusLocal: Authenticate users using the RADIUS server security database first. If the RADIUS server is unavailable, then use the local switch security database.
TotalServers	Number of RADIUS servers to configure during this session. Setting TotalServers to 0 disables all RADIUS authentication. The default is 0.
ServerIPAddress	IP address of the RADIUS server. The default is 10.0.0.1.
ServerUDPPort	User Datagram Protocol (UDP) port number on the RADIUS server. The default is 1812.
DeviceAuthServer	Enable (True) or disable (False) this server for device authentication. The default is False.

Table A-23. RADIUS Service Settings (Continued)

Entry	Description
UserAuthServer	Enable (True) or disable (False) this server for user account authentication. A user authentication RADIUS server requires a secure management connection (SSL). The default is True.
AccountingServer	Enable (True) or disable (False) this server for auditing of activity during a user session. When enabled, user activity is audited whether UserAuthServer is enabled or not.The default is False. The accounting server UDP port number is the ServerUDPPort value plus 1 (default 1813).
Timeout	Number of seconds to wait to receive a response from the RADIUS server before timing out. The default is 2.
Retries	Number of retries after the first attempt to establish communication with the RADIUS server fails. The default is 0.
SignPackets	Enable (True) or disable (False) the use of sign packets to protect the RADIUS server packet integrity. The default is False.
Secret	32-byte hex string or 16-byte ASCII string used as a password for authentication purposes between the switch and the RADIUS server.

services
Prompts you in a line-by-line fashion to enable or disable switch services. Table A-24 describes the switch service parameters. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Use caution when disabling TelnetEnabled and GUIMgmtEnabled; it is possible to disable all Ethernet access to the switch.

Table A-24. Switch Services Settings

Entry	Description
TelnetEnabled	Enables (True) or disables (False) the ability to manage the switch over a Telnet connection. Disabling this service is not recommended. The default is True.
SSHEnabled	Enables (True) or disables (False) Secure Shell (SSH) connections to the switch. SSH secures the remote connection to the switch. To establish a secure remote connection, your workstation must use an SSH client. The default is False.
GUIMgmtEnabled	Enables (True) or disables (False) out-of-band management of the switch with SANsurfer Switch Manager, the SANsurfer Switch Manager Application Application Programming Interface, SNMP, and CIM. If this service is disabled, the switch can only be managed inband or through the serial port. The default is True.
SSLMgmtEnabled	Enables (True) or disables (False) secure SSL connections for management applications including SANsurfer Switch Manager, the SANsurfer Switch Manager web applet, SANsurfer Switch Manager Application Programming Interface, and the CIM server. The default is False. ■ To enable secure SSL connections, you must first synchronize the date and time on the switch and workstation. ■ This service must be enabled to authenticate users through a RADIUS server. ■ Enabling SSL automatically creates a security certificate on the switch. ■ To disable SSL when using a user authentication RADIUS server, the RADIUS server authentication order must be local.

Table A-24. Switch Services Settings (Continued)

Entry	Description
EmbeddedGUIEnabled	Enables (True) or disables (False) the SANsurfer Switch Manager web applet. The web applet enables you to point at a switch with an internet browser and run SANsurfer Switch Manager through the browser. This parameter is the master control for the Set Setup System command parameter, EmbeddedGUIEnabled. The default is True.
SNMPEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Simple Network Management Protocol (SNMP). This parameter is the master control for the Set Setup SNMP command parameter, SNMPEnabled. The default is True.
NTPEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) which allows the synchronizing of switch and workstation dates and times with an NTP server. This helps to prevent invalid SSL certificates and timestamp confusion in the event log. The default is False. This parameter is the master control for the Set Setup System command parameter, NTPClientEnabled. The default is False.
CIMEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use the Common Information Model (CIM). The default is True.
FTPEnabled	Enables (True) or disables (False) the File Transfer Protocol (FTP) for transferring files rapidly between the workstation and the switch. The default is True.
MgmtServerEnabled	Enables (True) or disables (False) the management of the switch through third-party applications that use GS-3 Management Server (MS). This parameter is the master control for the Set Config Port command parameter, MSEnable. The default is False.

snmp
Prompts you in a line-by-line fashion to change SNMP configuration settings. Table A-25 describes the SNMP fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Table A-25. SNMP Configuration Settings

Entry	Description
SNMPEnabled	Enables (True) or disables (False) SNMP on the switch. The default is True.
Contact	Specifies the name of the person to be contacted to respond to trap events. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Location	Specifies the name of the switch location. The name can be up to 64 characters excluding #, semicolon (;), and comma (,). The default is undefined.
Trap [1-5] Address	Specifies the workstation IP address to which SNMP traps are sent. The default address for trap 1 is 10.0.0.254. The default address for traps 2–5 is 0.0.0.0. Addresses, other than 0.0.0.0, for all traps must be unique.
Trap [1-5] Port	Specifies the workstation port to which SNMP traps are sent. Valid workstation port numbers are 1–65535. The default is 162.
Trap [1-5] Severity	Specifies the severity level to use when monitoring trap events. The default is Warning.
Trap [1-5] Version	Specifies the SNMP version (1 or 2) to use in formatting traps. The default is 2.
Trap [1-5] Enabled	Specifies whether traps (event information) are enabled or disabled (default).
ReadCommunity	Read community password that authorizes an SNMP agent to read information from the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The read community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
WriteCommunity	Write community password that authorizes an SNMP agent to write information to the switch. This is a write-only field. The value on the switch and the SNMP management server must be the same. The write community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “private”.

Table A-25. SNMP Configuration Settings (Continued)

Entry	Description
TrapCommunity	Trap community password that authorizes an SNMP agent to receive traps. This is a write-only field. The value on the switch and the SNMP management server must be the same. The trap community password can be up to 32 characters excluding #, semicolon (;), and comma (,). The default is “public”.
AuthFailureTrap	Enables (True) or disables (False) the generation of traps in response to trap authentication failures. The default is False.
ProxyEnabled	Enables (True) or disables (False) SNMP communication with other switches in the fabric. The default is True.

system
Prompts you in a line-by-line fashion to change system configuration settings. Table A-26 describes the system configuration fields. For each parameter, enter a new value or press the Enter key to accept the current value shown in brackets.

Note: Changing the IP address will terminate all Ethernet management sessions.

Table A-26. System Configuration Settings

Entry	Description
Eth0NetworkDiscovery	Ethernet boot method: 1 - Static, 2 - Bootp, 3 - DHCP, 4 - RARP. The default is 1 - Static.
Eth0NetworkAddress	Ethernet Internet Protocol (IP) address. The default is 10.0.0.1.
Eth0NetworkMask	Ethernet subnet mask address.
Eth0GatewayAddress	Ethernet IP address gateway.
AdminTimeout	Amount of time in minutes the switch waits before terminating an idle Admin session. Zero (0) disables the time out threshold. The default is 30, the maximum is 1440.
InactivityTimeout	Amount of time in minutes the switch waits before terminating an idle Telnet command line interface session. Zero (0) disables the time out threshold. The default is 0, the maximum is 1440.

Table A-26. System Configuration Settings (Continued)

Entry	Description
LocalLogEnabled	Enables (True) or disables (False) the saving of log information on the switch. The default is True.
RemoteLogEnabled	Enables (True) or disables (False) the recording of the switch event log on a remote host that supports the syslog protocol. The default is False.
RemoteLogHostAddress	The IP address of the host that will receive the switch event log information if remote logging is enabled. The default is 10.0.0.254.
NTPClientEnabled	Enables (True) or disables (False) the Network Time Protocol (NTP) client on the switch. This client enables the switch to synchronize its time with an NTP server. This feature supports NTP version 4 and is compatible with version 3. An Ethernet connection to the server is required and you must first set an initial time and date on the switch. The synchronized time becomes effective immediately. The default is False.
NTPServerAddress	The IP address of the NTP server from which the NTP client acquires the time and date. The default is 10.0.0.254.
EmbeddedGUIEnabled	Enables (True) or disables (False) the SANsurfer Switch Manager Web applet. Changing this parameter to False while the applet is running will terminate the applet. The default is True.

Examples

The following is an example of the Set Setup RADIUS command:

```
SANbox Manager (admin) #> set setup radius

  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the attributes
  for the server being processed, press 'q' or 'Q' and the ENTER key to do so.
  If you wish to terminate the configuration process completely, press 'qq' or
  'QQ' and the ENTER key to so do.

  DeviceAuthOrder   (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  UserAuthOrder     (1=Local, 2=Radius, 3=RadiusLocal) [Local]
  TotalServers      (decimal value, 0-5)               [1    ]

  Server: 1
  ServerIPAddress   (dot-notated IP Address)         [10.20.11.8]
  ServerUDPPort     (decimal value)                  [1812      ]
  DeviceAuthServer  (True / False)                   [True      ]
  UserAuthServer    (True / False)                   [True      ]
  AccountingServer  (True / False)                   [False     ]
  Timeout           (decimal value, 10-30 secs)      [10        ]
  Retries           (decimal value, 1-3, 0=None)     [0         ]
  SignPackets       (True / False)                   [False     ]
  Secret            (32 hex or 16 ASCII char value)  [********  ]
  Do you want to save and activate this radius setup? (y/n): [n]
```

The following is an example of the Set Setup Services command:

```
SANbox Manager (admin) #> set setup services

A list of attributes with formatting and current values will follow.
Enter a new value or simply press the ENTER key to accept the current value.
If you wish to terminate this process before reaching the end of the list
press 'q' or 'Q' and the ENTER key to do so.

*Warning: If services are disabled, the connection to the switch may be lost.


TelnetEnabled       (True / False)       [True ]
SSHEnabled          (True / False)       [False]
GUIMgmtEnabled      (True / False)       [True ]
SSLMgmtEnabled      (True / False)       [False]
EmbeddedGUIEnabled  (True / False)       [True ]
SNMPEnabled         (True / False)       [True ]
NTPEnabled          (True / False)       [False]
CIMEnabled          (True / False)       [True ]
FTPEnabled          (True / False)       [True ]
MgmtServerEnabled   (True / False)       [True ]


Do you want to save and activate this services setup? (y/n): [n]
```

The following is an example of the Set Setup SNMP command:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> set setup snmp
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.
  Trap Severity Options
  ---------------------
  unknown, emergency, alert, critical, error, warning, notify, info, debug, mark
  SNMPEnabled         (True / False)               [True             ]
  Contact             (string, max=64 chars)      [<sysContact undefined]
  Location            (string, max=64 chars)      [sysLocation undefined]
  Trap1Address        (dot-notated IP Address)    [10.20.71.15      ]
  Trap1Port           (decimal value)             [162              ]
  Trap1Severity       (see allowed options above) [warning          ]
  Trap1Version        (1 / 2)                     [2                ]
  Trap1Enabled        (True / False)              [False            ]
  Trap2Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap2Port           (decimal value)             [162              ]
  Trap2Severity       (see allowed options above) [warning          ]
  Trap2Version        (1 / 2)                     [2                ]
  Trap2Enabled        (True / False)              [False            ]
  Trap3Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap3Port           (decimal value)             [162              ]
  Trap3Severity       (see allowed options above) [warning          ]
  Trap3Version        (1 / 2)                     [2                ]
  Trap3Enabled        (True / False)              [False            ]
  Trap4Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap4Port           (decimal value)             [162              ]
  Trap4Severity       (see allowed options above) [warning          ]
  Trap4Version        (1 / 2)                     [2                ]
  Trap4Enabled        (True / False)              [False            ]
  Trap5Address        (dot-notated IP Address)    [0.0.0.0          ]
  Trap5Port           (decimal value)             [162              ]
  Trap5Severity       (see allowed options above) [warning          ]
  Trap5Version        (1 / 2)                     [2                ]
  Trap5Enabled        (True / False)              [False            ]
  ReadCommunity       (string, max=32 chars)      [public           ]
  WriteCommunity      (string, max=32 chars)      [private          ]
  TrapCommunity       (string, max=32 chars)      [public           ]
  AuthFailureTrap     (True / False)              [False            ]
  ProxyEnabled        (True / False)              [True             ]
```

The following is an example of the Set Setup System command:

```
SANbox Manager (admin) #> set setup system
  A list of attributes with formatting and current values will follow.
  Enter a new value or simply press the ENTER key to accept the current value.
  If you wish to terminate this process before reaching the end of the list
  press 'q' or 'Q' and the ENTER key to do so.

Eth0NetworkDiscovery    (1=Static, 2=Bootp, 3=Dhcp, 4=Rarp)  [Static       ]
Eth0NetworkAddress      (dot-notated IP Address)             [10.0.0.1     ]
Eth0NetworkMask         (dot-notated IP Address)             [255.255.255.0]
Eth0GatewayAddress      (dot-notated IP Address)             [10.0.0.254   ]
AdminTimeout            (dec value 0-1440 minutes, 0=never)  [30           ]
InactivityTimeout       (dec value 0-1440 minutes, 0=never)  [0            ]
LocalLogEnabled         (True / False)                       [True         ]
RemoteLogEnabled        (True / False)                       [False        ]
RemoteLogHostAddress    (dot-notated IP Address)             [10.0.0.254   ]
NTPClientEnabled        (True / False)                       [False        ]
NTPServerAddress        (dot-notated IP Address)             [10.0.0.254   ]
EmbeddedGUIEnabled      (True / False)                       [True         ]
```

Show Command

Displays fabric, switch, and port operational information.

Authority None

Syntax **show**

about
alarm *[option]*
audit
broadcast
chassis
cimlistener *[listener_name]*
cimsubscription *[subscription_name]*
config [option]
domains
donor
fabric
fdmi *[port_wwn]*
interface
log *[option]*
lsdb
mem [count]
ns *[option]*
pagebreak
perf *[option]*
port *[port_number]*
post log
setup [option]
steering *[domain_id]*
support
switch
timezone
topology
users
version

Keywords **about**

Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the Version keyword.

alarm *[option]*
Displays the alarm log and session display setting. If you omit [option], the command displays the last 200 alarm entries. The alarm log is cleared when the switch is reset or power cycled. [option] has the following value:

setting
Displays the status of the parameter that controls the display of alarms in the session output stream. This parameter is set using the Set Alarm command.

audit
Displays the most recent 200 records in the administrative audit log. The audit log contains configuration and administrative changes that have been made to the switch including the originating management session and IP address.

broadcast
Displays the broadcast tree information and all ports that are currently transmitting and receiving broadcast frames.

chassis
Displays chassis component status and temperature.

cimlistener *[listener_name]*
Displays CIM indicator services listener information for the listener given by [listener_name]. If you omit [listener_name], the command displays all listeners.

cimsubscription *[subscription_name]*
Displays CIM subscription information for the subscription given by [subscription_name]. If you omit [subscription_name], the command displays all subscriptions.

config [option]
Displays switch, port, and zoning configuration attributes. Refer to the ”Show Config Command” on page A-106.

domains
Displays list of each domain and its worldwide name in the fabric.

donor
Displays list of current donor configuration for all ports.

fabric
Displays list of each domain, symbolic name, worldwide name, node IP address, and port IP address.

fdmi *[port_wwn]*
Displays detailed information about the device host bus adapter given by [port_wwn]. If you omit [port_wwn], the command displays a summary of host bus adapter information for all attached devices in the fabric. Illegal characters in the display appear as question marks (?).

interface
Displays the status of the active network interfaces.

log *[option]*
Displays log entries. Refer to the ”Show Log Command” on page A-109. The log is cleared when the switch is reset or power cycled.

lsdb
Displays Link State database information

mem [count]
Displays information about memory activity for the number of seconds given by [count]. If you omit [count], the value 1 is used. Displayed memory values are in 1K block units.

> ***Note:*** This keyword will display memory activity updates until [count] is reached – it cannot be interrupted. Therefore, avoid using large values for [count].

ns *[option]*
Displays name server information for the specified [option]. If you omit [option], name server information for the local domain ID is displayed. [option] can have the following values:

all
Displays name server information for all switches and ports.

[domain_id]
Displays name server information for the switch given by [domain_id]. [domain_id] is a switch domain ID.

[port_id]
Displays name server information for the port given by [port_id]. [port_id] is a port Fibre Channel address.

pagebreak
Displays the current pagebreak setting. The pagebreak setting limits the display of information to 20 lines (On) or allows the continuous display of information without a break (Off).

perf *[option]*
Displays performance information for all ports. Refer to the ”Show Perf Command” on page A-112.

port *[port_number]*
Displays operational information for the port given by [port_number]. Ports are numbered beginning with 0. If [port number] is omitted, information is displayed for all ports. Table A-27 describes the port parameters.

Table A-27. Show Port Parameters

Entry	Description
AInit	Incremented each time the port begins AL initialization.
AInitError	Number of times the port entered initialization and the initialization failed.
Bad Frames	Number of frames that have framing errors.
ClassXFramesIn	Number of class *x* frames received by this port.
ClassXFramesOut	Number of class *x* frames sent by this port.
ClassXWordsIn	Number of class *x* words received by this port.
ClassXWordsOut	Number of class *x* words sent by this port.
ClassXToss	Number of times an SOFi3 or SOFn3 frame is tossed from TBUF.
DecodeError	Number of decode errors detected
EpConnects	Number of times an E_Port connected through ISL negotiation.
FBusy	Number of times the switch sent a F_BSY because Class 2 frame could not be delivered within ED_TOV time. Number of class 2 and class 3 fabric busy (F_BSY) frames generated by this port in response to incoming frames. This usually indicates a busy condition on the fabric or N_Port that is preventing delivery of this frame.
Flowerrors	Received a frame when there were no available credits.
FReject	Number of frames from devices that were rejected.
InvalidCRC	Invalid CRC detected.
InvalidDestAddr	Invalid destination address detected.
LIP_AL_PD_ALPS	Number of F7, AL_PS LIPs, or AL_PD (vendor specific) resets, performed.
LIP_F7_AL_PS	This LIP is used to reinitialize the loop. An L_Port, identified by AL_PS, may have noticed a performance degradation and is trying to restore the loop.

Table A-27. Show Port Parameters (Continued)

Entry	Description
LIP_F8_AL_PS	This LIP denotes a loop failure detected by the L_Port identified by AL_PS.
LIP_F7_F7	A loop initialization primitive frame used to acquire a valid AL_PA.
LIP_F8_F7	A loop initialization primitive frame used to indicate that a loop failure has been detected at the receiver.
Link Failures	Number of optical link failures detected by this port. A link failure is a loss of synchronization or a loss of signal while not in the offline state. A loss of signal causes the switch to attempt to re-establish the link. If the link is not re-established, a link failure is counted. A link reset is performed after a link failure.
Login	Number of device logins
Logout	Number of device logouts
LoopTimeouts	A two (2) second timeout as specified by FC-AL-2.
LossOfSync	Number of synchronization losses (>100 ms) detected by this port. A loss of synchronization is detected by receipt of an invalid transmission word.
PrimSeqErrors	Primitive sequence errors detected.
RxLinkResets	Number of link reset primitives received from an attached device.
RxOfflineSeq	Number of offline sequences received. An OLS is issued for link initialization, a Receive & Recognize Not_Operational (NOS) state, or to enter the offline state.
TotalErrors	Total number of errors detected.
TotalLIPsRecvd	Number of loop initialization primitive frames received by this port.
TotalLIPsXmitd	Number of loop initialization primitive frames transmitted by this port.
TotalLinkResets	Total number of link reset primitives.
TotalOfflineSeq	Total number of Offline Sequences issued and received by this port.
TotalRxFrames	Total number of frames received by this port.
TotalRxWords	Total number of words received by this port.

Table A-27. Show Port Parameters (Continued)

Entry	Description
TotalTxFrames	Total number of frames issued by this port.
TotalTxWords	Total number of words issued by this port.
TxLinkResets	Number of Link Resets issued by this port.
TxOfflineSeq	Total number of Offline Sequences issued by this port.

post log
Displays the Power On Self Test (POST) log which contains results from the most recently failed POST.

setup [option]
Displays setup attributes for the system, SNMP, and the switch manufacturer. Refer to the ”Show Setup Command” on page A-114.

steering *[domain_id]*
Displays the routes that data takes to the switch given by [domain_id]. If you omit [domain_id], the system displays routes for all switches in the fabric.

support
Executes a series of commands that display a complete description of the switch, its configuration, and operation. The display can be captured from the screen and used for diagnosing problems. This keyword is intended for use at the request of your authorized maintenance provider. The commands that are executed include the following:

- Alias List
- Config List
- Date
- Group List
- History
- Ps
- Security (List, Limits, History)
- Securityset (Active, List)
- Show (About, Alarm, Backtrace, Chassis, Config Port, Config Security, Config Switch, Config Threshold, Dev, Dev Settings, Domains, Donor, Fabric, Log, Log Archive, Log Settings, Lsdb, Mem, Ns, Perf, Port, Setup Mfg, Setup Snmp, Setup System, Steering, Switch, Topology, Users)
- Uptime
- User Accounts

- Whoami
- Zoneset (Active, List)
- Zoning (History, Limits, List)

switch
Displays switch operational information.Table A-28 describes the switch operational parameters.

Table A-28. Switch Operational Parameters

Parameter	Description
SymbolicName	Descriptive name for the switch
SwitchWWN	Switch world wide name
SwitchType	Switch model
BootVersion	PROM boot version
CreditPool	Number of port buffer credits available to recipient ports
DomainID	Switch domain ID
FirstPortAddress	FC address of switch port 0
FlashSize - MBytes	Size of the flash memory in megabytes
LogLevel	Event severity level used to record events in the event log
MaxPorts	Number of ports available on the switch
NumberOfResets	Number of times the switch has been reset over its service life
ReasonForLastReset	Action that caused the last reset
ActiveImageVersion - build date	Active firmware image version and build date.
PendingImageVersion - build date	Firmware image version and build date that is pending. This image will become active at the next reset or power cycle.
ActiveConfiguration	Name of the switch configuration that is in use.
AdminState	Switch administrative state
AdminModeActive	Admin session status

Table A-28. Switch Operational Parameters (Continued)

Parameter	Description
BeaconOnStatus	Beacon status as set by the Set Beacon command.
OperationalState	Switch operational state
PrincipalSwitchRole	Principal switch status. True indicates that this switch is the principal switch.
BoardTemp (1) - Degrees Celsius	Internal switch temperature at circuit board sensor 1
SwitchDiagnosticsStatus	Results of the power-on self test
SwitchTemperatureStatus	Switch temperature status: normal, warning, failure

timezone
Displays the current time zone setting.

topology
Displays all connected devices.

users
Displays a list of logged-in users. This is equivalent to the User List command.

version
Displays an introductory set of information about operational attributes of the switch. This keyword is equivalent to the About keyword.

Examples

The following is an example of the Show Chassis command:

```
SANbox Manager #> show chassis
  Chassis Information
  -------------------
  BoardTemp (1) - Degrees Celsius   36
  FanStatus (1)                     Good
  FanStatus (2)                     Good
  FanDirection (1)                  BackToFront
  FanDirection (2)                  BackToFront
  PowerSupplyStatus (1)             Good
  PowerSupplyStatus (2)             Good
  HeartBeatCode                     1
  HeartBeatStatus                   Normal
```

The following is an example of the Show Domains command:

```
SANbox Manager #> show domains
  Principal switch is (remote): 10:00:00:60:69:50:0b:6c
  Upstream Principal ISL is   : 1
  Domain ID List:
        Domain 97  (0x61)  WWN = 10:00:00:c0:dd:00:71:ed
        Domain 98  (0x62)  WWN = 10:00:00:60:df:22:2e:0c
        Domain 99  (0x63)  WWN = 10:00:00:c0:dd:00:72:45
        Domain 100 (0x64)  WWN = 10:00:00:c0:dd:00:ba:68
        Domain 101 (0x65)  WWN = 10:00:00:60:df:22:2e:06
        Domain 102 (0x66)  WWN = 10:00:00:c0:dd:00:90:ef
        Domain 103 (0x67)  WWN = 10:00:00:60:69:50:0b:6c
        Domain 104 (0x68)  WWN = 10:00:00:c0:dd:00:b8:b7
```

The following is an example of the Show Fabric command:

```
SANbox Manager #> show fabric

 Domain     WWN                     Enet IP Addr    FC IP Addr      SymbolicName
 ------     ---                     ------------    ----------      ------------
 16 (0x10)  10:00:00:c0:dd:00:77:81 10.20.68.11     0.0.0.0         gui sb1 .11
 17 (0x11)  10:00:00:c0:dd:00:6a:2d 10.20.68.12     0.0.0.0         sw12
 18 (0x12)  10:00:00:c0:dd:00:c3:04 10.20.68.160    0.0.0.0         sw .160
 19 (0x13)  10:00:00:c0:dd:00:bc:56 10.20.68.108    0.0.0.0         Sb2 .108
```

The following is an example of the Show FDMI command:

```
SANbox Manager #> show fdmi

HBA ID                  PortID  Manufacturer           Model    Ports
--------                ------  ---------------       -------  -----
21:01:00:e0:8b:27:aa:bc 610000  QLogic Corporation    QLA2342  2
21:00:00:00:ca:25:9b:96 180100  QLogic Corporation    QL2330   2
```

The following is an example of the Show FDMI WWN command:

```
SANbox Manager #> show fdmi 21:00:00:e0:8b:09:3b:17
  FDMI Information
  ----------------
  Manufacturer            QLogic Corporation
  SerialNumber            [04202
  Model                   QLA2342
  ModelDescription        QLogic QLA2342 PCI Fibre Channel Adapter
  PortID                  610000
  NodeWWN                 20:00:00:e0:8b:07:aa:bc
  HardwareVersion         FC5010409-10
  DriverVersion           8.2.3.10 Beta 2 (W2K VI)
  OptionRomVersion        1.21
  FirmwareVersion         03.02.13.
  OperatingSystem         SunOS 5.8
  MaximumCTPayload        2040
  NumberOfPorts           1

  Port  21:01:00:e0:8b:27:aa:bc

  SupportedFC4Types       FCP
  SupportedSpeed          2Gb/s
  CurrentSpeed            2Gb/s
  MaximumFrameSize        2048
  OSDeviceName
  HostName
```

The following is an example of the Show NS (local domain) command:

```
SANbox Manager #> show ns
  Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   19 (0x13) 1301e1 NL   3   21:00:00:20:37:73:13:69 20:00:00:20:37:73:13:69
  2   19 (0x13) 1301e2 NL   3   21:00:00:20:37:73:12:9b 20:00:00:20:37:73:12:9b
  3   19 (0x13) 1301e4 NL   3   21:00:00:20:37:73:05:26 20:00:00:20:37:73:05:26
  4   19 (0x13) 130d00 N    3   21:01:00:e0:8b:27:a7:bc 20:01:00:e0:8b:27:a7:bc
```

The following is an example of the Show NS [domain_ID] command:

```
SANbox Manager #> show ns 18
    Seq Domain    Port   Port
  No  ID        ID     Type COS PortWWN                 NodeWWN
  --- ------    ------ ---- --- -------                 -------
  1   18 (0x12) 120700 N    3   21:00:00:e0:8b:07:a7:bc 20:00:00:e0:8b:07:a7:bc
```

The following is an example of the Show NS [port_ID] command:

```
SANbox Manager #> show ns 1301e1
  Port ID: 1301e1
  --------
  PortType          NL
  PortWWN           21:00:00:20:37:73:13:69
  SymbolicPortName
  NodeWWN           20:00:00:20:37:73:13:69
  SymbolicNodeName
  NodeIPAddress     0.0.0.0
  ClassOfService    3
  PortIPAddress     0.0.0.0
  FabricPortName    20:01:00:c0:dd:00:bc:56
  FC4Type           FCP
  FC4Desc           (NULL)
```

The following is an example of the Show Interface command:

```
SANbox Manager #> show interface
eth0      Link encap:Ethernet  HWaddr 00:C0:DD:00:BD:ED
          inet addr:10.20.68.107  Bcast:10.20.68.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4712 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:415313 (405.5 Kb)  TX bytes:716751 (699.9 Kb)
          Interrupt:11 Base address:0xfcc0
lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:304 errors:0 dropped:0 overruns:0 frame:0
          TX packets:304 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:20116 (19.6 Kb)  TX bytes:20116 (19.6 Kb)
```

The following is an example of the Show Port command:

```
SANbox Manager #> show port 1
  Port Number: 1
  ------------
  AdminState       Online             OperationalState Online
  AsicNumber       0                  PerfTuningMode   Normal
  AsicPort         1                  PortID           0e0800
  ConfigType       GL                 PortWWN          20:08:00:c0:dd:03:d5:94
  DiagStatus       Passed             RunningType      E
  EpConnState      Connected          MediaPartNumber  PL-XPL-VC-SG3-22
  EpIsoReason      NotApplicable      MediaRevision    1
  IOStreamGuard    Disabled           MediaType        400-M5-SN-I
  LinkSpeed        2Gb/s              MediaVendor      Unknown
  LinkState        Active             MediaVendorID    00000485
  LoginStatus      LoggedIn           SymbolicName     Port8

  ALInit          5                    LIP_F8_AL_PS    0
  ALInitError     0                    LIP_F8_F7       0
  BadFrames       0                    LinkFailures    2
  Class2FramesIn  0                    Login           3
  Class2FramesOut 0                    Logout          2
  Class2WordsIn   0                    LoopTimeouts    1
  Class2WordsOut  0                    LossOfSync      2
  Class3FramesIn  999                  PrimSeqErrors   0
  Class3FramesOut 540                  RxLinkResets    1
  Class3Toss      0                    RxOfflineSeq    0
  Class3WordsIn   29516                TotalErrors     628777
  Class3WordsOut  8406                 TotalLinkResets 6
  DecodeErrors    628775               TotalLIPsRecvd  5
  EpConnects      3                    TotalLIPsXmitd  7
  FBusy           0                    TotalOfflineSeq 5
  FlowErrors      0                    TotalRxFrames   999
  FReject         0                    TotalRxWords    29516
  InvalidCRC      0                    TotalTxFrames   540
  InvalidDestAddr 0                    TotalTxWords    8406
  LIP_AL_PD_AL_PS 0                    TxLinkResets    5
  LIP_F7_AL_PS    0                    TxOfflineSeq    5
  LIP_F7_F7       5
```

The following is an example of the Show Switch command:

```
SANbox Manager #> show switch
Switch Information
------------------
SymbolicName                     sw .108
SwitchWWN                        100000c0dd00bc56
SwitchType                       SANbox 5602
BootVersion                      Vx.x.x.x-0 (day month date time year)
CreditPool                       0
DomainID                         19 (0x13)
FirstPortAddress                 130000
FlashSize - MBytes               128
LogLevel                         Critical
NumberOfResets                   15
ReasonForLastReset               PowerUp
ActiveImageVersion - build date  Vx.x.x.0-2 (day month date time year)
PendingImageVersion - build date Vx.x.x.0-17 (day month date time year)
ActiveConfiguration              default
AdminState                       Online
AdminModeActive                  False
BeaconOnStatus                   False
OperationalState                 Online
PrincipalSwitchRole              False
BoardTemp (1) - Degrees Celsius  32
SwitchDiagnosticsStatus          Passed
SwitchTemperatureStatus          Normal
```

The following is an example of the Show Topology command:

```
SANbox Manager #> show topology
Unique ID Key
-------------
A = ALPA,  D = Domain ID,  P = Port ID
Port   Local Local                    Remote  Remote                    Unique
Number Type  PortWWN                  Type    NodeWWN                   ID
------ ----- -------                  ------  -------                   ------
5      F     20:05:00:c0:dd:00:bd:ec   N      20:00:00:00:c9:22:1e:93   010500 P
10     E     20:0a:00:c0:dd:00:bd:ec   E      10:00:00:c0:dd:00:80:21   4(0x4) D
```

The following is an example of the Show Topology command for port 1:

```
SANbox Manager  #> show topology 1
  Local Link Information
  ----------------------
  PortNumber 1
  PortID     650100
  PortWWN    20:01:00:c0:dd:00:91:11
  PortType   F

Remote Link Information
-----------------------
Device 0
NodeWWN 50:80:02:00:00:06:d5:38
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 1
NodeWWN 20:00:00:20:37:2b:08:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0

Device 2
Description (NULL)
IPAddress 0.0.0.0

Device 3
NodeWWN 20:00:00:20:37:2b:05:c9
PortType NL
Description (NULL)
IPAddress 0.0.0.0
```

The following is an example of the Show Version command:

```
SANbox Manager #> show version
       ***************************************************
       *                                                 *
       *       Command Line Interface SHell  (CLISH)     *
       *                                                 *
       ***************************************************

       SystemDescription     SANbox 5602 FC Switch
       Eth0NetworkAddress    10.20.11.192 (use 'set setup system' to update)
       MACAddress            00:c0:dd:00:71:ee
       WorldWideName         10:00:00:c0:dd:00:71:ed
       ChassisSerialNumber   FAM033100024
       SymbolicName          SANbox Manager
       ActiveSWVersion       V5.0.x.x.xx.xx
       ActiveTimestamp       day month date time year
       DiagnosticsStatus     Passed
```

Show Config Command

Displays switch, port, alarm threshold, security, and zoning for the current configuration.

Authority None

Syntax **show config**
port *[port_number]*
security
switch
threshold
zoning

Keywords **port *[port_number]***
Displays configuration parameters for the port number given by [port_number]. Ports are numbered beginning with 0. If [port_number] is omitted, all ports are specified.

security
Displays the security database Autosave parameter value.

switch
Displays configuration parameters for the switch.

threshold
Displays alarm threshold parameters for the switch.

zoning
Displays zoning configuration parameters for the switch.

Examples The following is an example of the Show Config Port command:

```
SANbox Manager #> show config port 3

    Port Number: 3
  ------------
  AdminState         Offline
  LinkSpeed          Auto
  PortType           GL
  SymbolicName       Port3
  ALFairness         False
  DeviceScanEnabled  True
  ForceOfflineRSCN   False
  ARB_FF             False
  InteropCredit      0
  ExtCredit          0
  FANEnabled         True
  AutoPerfTuning     False
  LCFEnabled         False
  MFSEnabled         True
```

```
 MSEnabled          True
 NoClose            False
 IOStreamGuard      Disabled
 VIEnabled          False
 PDISCPingEnable    True
```

The following is an example of the Show Config Switch command:

```
SANbox Manager #> show config switch
 Configuration Name: default
 -------------------
  Switch Configuration Information
  --------------------------------
  AdminState            Online
  BroadcastEnabled      False
  InbandEnabled         True
  FDMIEnabled           False
  FDMIEntries           10
  DomainID              19 (0x13)
  DomainIDLock          True
  SymbolicName          sw108
  R_A_TOV               10000
  E_D_TOV               2000
  PrincipalPriority     254
  ConfigDescription     Default Config
  ConfigLastSavedBy     admin@OB-session5
  ConfigLastSavedOn     day month date time year
  InteropMode           Standard
```

The following is an example of the Show Config Threshold command:

```
SANbox Manager #> show config threshold
Configuration Name: default
------------
  Threshold Configuration Information
-----------------------------------
ThresholdMonitoringEnabled    False
CRCErrorsMonitoringEnabled    True
RisingTrigger                 25
FallingTrigger                1
SampleWindow                  10
DecodeErrorsMonitoringEnabled True
RisingTrigger                 25
FallingTrigger                0
SampleWindow                  10
ISLMonitoringEnabled          True
RisingTrigger                 2
FallingTrigger                0
SampleWindow                  10
LoginMonitoringEnabled        True
RisingTrigger                 5
FallingTrigger                1
SampleWindow                  10
LogoutMonitoringEnabled       True
RisingTrigger                 5
FallingTrigger                1
SampleWindow                  10
LOSMonitoringEnabled          True
RisingTrigger                 100
FallingTrigger                5
SampleWindow                  10
```

The following is an example of the Show Config Zoning command:

```
SANbox Manager #> show config zoning
 Configuration Name: default
  -------------------
  Zoning Configuration Information
  --------------------------------
  InteropAutoSave       True
  DefaultVisibility     All
  DiscardInactive       False
```

Show Log Command

Displays the contents of the log or the parameters used to create and display entries in the log. The log contains a maximum of 1200 entries. When the log reaches its entry capacity, subsequent entries overwrite the existing entries, beginning with the oldest.

Authority None

Syntax **show log**
[number_of_events]
component
display [filter]
level
options
port
settings

Keywords **[number_of_events]**
Specifies the number of the most recent events to display from the event log. [number_of_events] must be a positive integer.

component
Displays the components currently being monitored for events. The components are as follows:

All
Monitors all components.

Chassis
Monitors chassis hardware components such as fans and power supplies.

Eport
Monitors all E_Ports.

Mgmtserver
Monitors management server status.

Nameserver
Monitors name server status.

None
Monitor none of the component events.

Other
Monitors other miscellaneous events.

Port
Monitors all port events

SNMP
SNMP events.

Switch
Monitors switch management events.

Zoning
Monitors zoning conflict events.

display [filter]
Displays log events on the screen according to the component or severity level filter given by [filter]. [filter] can be one of the following:

Info
Displays all informative events.

Warning
Displays all warning events.

Critical
Displays all critical events.

Eport
Displays all events related to E_Ports.

Mgmtserver
Displays all events related to the management server.

Nameserver
Displays all events related to the name server.

Port [port_number]
Displays all events related to the port given by [port_number].

SNMP
Displays all events related to SNMP.

Switch
Displays all events related to switch management.

Zoning
Displays all events related to zoning.

level
Displays the event severity level logging setting and the display level setting.

options
Displays the options that are available for configuring event logging and automatic display to the screen. Refer to the for information about how to configure event logging and display level.

port
Displays the ports being monitored for events. If an event occurs which is of the defined level and on a defined component, but not on a defined port, no entry is made in the log.

settings
Displays the current filter settings for component, severity level, port, and display level. This command is equivalent to executing the following commands separately: Show Log Component, Show Log Level, and Show Log Port.

Examples

The following is an example of the Show Log Component command:

```
SANbox Manager #> show log component
Current settings for log
   ------------------------
   FilterComponent   NameServer MgmtServer Zoning Switch Blade Port Eport Snmp
```

The following is an example of the Show Log Level command:

```
SANbox Manager #> show log level
   Current settings for log
   ------------------------
   FilterLevel       Info
   DisplayLevel      Critical
```

The following is an example of the Show Log Options command:

```
SANbox Manager #> show log options
  Allowed options for log
  -----------------------
   FilterComponent
All,None,NameServer,MgmtServer,Zoning,Switch,Blade,Port,Eport,Snmp
   FilterLevel       Critical,Warn,Info,None
   DisplayLevel      Critical,Warn,Info,None
```

The following is an example of the Show Log command:

```
  SANbox Manager #> show log
   [327][day month date time year][I][Eport Port:0/8][Eport State=
   E_A0_GET_DOMAIN_ID]
   [328][day month date time year][I][Eport Port: 0/8][FSPF PortUp state=0]
   [329][day month date time year][I][Eport Port: 0/8][Sending init hello]
   [330][day month date time year][I][Eport Port: 0/8][Processing EFP, oxid= 0x8]
   [331][day month date time year][I][Eport Port: 0/8][Eport State = E_A2_IDLE]
   [332][day month date time year][I][Eport Port: 0/8][EFP,WWN= 0x100000c0dd00b845,
   len= 0x30]
   [333][day month date time year][I][Eport Port: 0/8][Sending LSU oxid=0xc:type=1]
   [334][day month date time year][I][Eport Port: 0/8][Send Zone Merge Request]
   [335][day month date time year][I][Eport Port: 0/8][LSDB Xchg timer set]
   [336][day month date time year][I][Eport Port: 0/8][Setting attribute
   Oper.UserPort.0.8.EpConnState Connected]
```

Show Perf Command

Displays port performance in frames/second and bytes/second. If you omit the keyword, the command displays data transmitted (out), data received (in), and total data transmitted and received in frames/second and bytes per second.

Authority None

Syntax **show perf**

byte *[port_number]*
inbyte *[port_number]*
outbyte *[port_number]*
frame *[port_number]*
inframe *[port_number]*
outframe *[port_number]*
errors *[port_number]*

Keywords ***[port_number]***

Displays continuous performance data in total bytes/second transmitted and received for the port group (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

[port_number]

Displays continuous performance data in bytes/second received for the port group (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

[port_number]

Displays continuous performance data in bytes/second transmitted for the set of 16 ports (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

[port_number]

Displays continuous performance data in total frames/second transmitted and received for the set of 16 ports (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

[port_number]

Displays continuous performance data in frames/second received for the port group (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

[port_number]

Displays continuous performance data in frames/second transmitted for the port group (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

[port_number]
Displays continuous error counts for the port group (0–15 or 16–19) that includes [port_number]. If you omit [port_number], ports 0–15 are displayed. Type “q” and press the Enter key to stop the display.

Examples

The following is an example of the Show Perf command:

```
SANbox Manager #> show perf
Port   Bytes/s    Bytes/s    Bytes/s    Frames/s   Frames/s   Frames/s
  Number   (in)       (out)    (total)      (in)       (out)    (total)
  ------ -------    -------    -------    --------   --------   --------
  0      7K         136M       136M       245        68K        68K
  1      58K        0          58K        1K         0          1K
  2      0          0          0          0          0          0
  3      0          0          0          0          0          0
  4      0          0          0          0          0          0
  5      0          0          0          0          0          0
  6      0          7K         7K         0          245        245
  7      136M       58K        136M       68K        1K         70K
  8      7K         136M       136M       245        68K        68K
  9      58K        0          58K        1K         0          1K
  10     0          0          0          0          0          0
  11     0          0          0          0          0          0
  12     0          0          0          0          0          0
  13     0          0          0          0          0          0
  14     0          7K         7K         0          245        245
  15     136M       58K        136M       68K        1K         70K
  16     47M        23K        47M        23K        726        24K
  17     0          0          0          0          0          0
  18     23K        47M        47M        726        23K        24K
  19     0          0          0          0          0          0
```

The following is an example of the Show Perf Byte command:

Show Setup Command

Displays the current SNMP and system settings.

Authority None

Syntax **show setup**
mfg
radius
services
snmp
system

Keywords **mfg**
Displays manufacturing information about the switch.

radius
Displays RADIUS server information.

services
Displays switch service status information.

snmp
Displays the current SNMP settings.

system
Displays the current system settings.

Examples The following is an example of the Show Setup Mfg command:

```
SANbox Manager #> show setup mfg
```

The following is an example of the Show Setup Services command:

```
SANbox Manager #> show setup services
System Services
----------------------------
TelnetEnabled             True
SSHEnabled                False
GUIMgmtEnabled            True
SSLMgmtEnabled            False
EmbeddedGUIEnabled        True
SNMPEnabled               True
NTPEnabled                True
CIMEnabled                True
FTPEnabled                True
ManagementServerEnabled   True
```

The following is an example of the Show Setup RADIUS command:

```
SANbox Manager #> show setup radius

  Radius Information
  ------------------
  DeviceAuthOrder   RadiusLocal
  UserAuthOrder     RadiusLocal
  TotalServers      1

  Server: 1

  ServerIPAddress   10.20.11.8
  ServerUDPPort     1812
  DeviceAuthServer  False
  UserAuthServer    True
  AccountingServer  False
  Timeout           2
  Retries           0
  SignPackets       False
  Secret            ********
```

The following is an example of the Show Setup Snmp command:

```
SANbox Manager #> show setup snmp
  SNMP Information
  ----------------
  SNMPEnabled           True
  Contact               <sysContact undefined>
  Location              N_107 System Test Lab
  Description           SANbox 5602 FC Switch
  Trap1Address          10.0.0.254
  Trap1Port             162
  Trap1Severity         warning
  Trap1Version          2
  Trap1Enabled          False
  Trap2Address          0.0.0.0
  Trap2Port             162
  Trap2Severity         warning
  Trap2Version          2
  Trap2Enabled          False
  Trap3Address          0.0.0.0
  Trap3Port             162
  Trap3Severity         warning
  Trap3Version          2
  Trap3Enabled          False
  Trap4Address          0.0.0.0
  Trap4Port             162
  Trap4Severity         warning
  Trap4Version          2
  Trap4Enabled          False
  Trap5Address          0.0.0.0
  Trap5Port             162
  Trap5Severity         warning
  Trap5Version          2
  Trap5Enabled          False
  AuthFailureTrap       True
  ProxyEnabled          True
```

The following is an example of the Show Setup System command:

```
SANbox Manager #> show setup system
  System Information
  ------------------
  Eth0NetworkDiscovery     Static
  Eth0NetworkAddress       10.20.11.32
  Eth0NetworkMask          255.255.252.0
  Eth0GatewayAddress       10.20.8.254
  AdminTimeout             30
  InactivityTimeout        0
  LocalLogEnabled          True
  RemoteLogEnabled         False
  RemoteLogHostAddress     10.0.0.254
  NTPClientEnabled         True
  NTPServerAddress         51.68.85.102
  EmbeddedGUIEnabled       True
```

Shutdown Command

Terminates all data transfers on the switch at convenient points and closes the Telnet session. Always power cycle the switch after entering this command.

Authority Admin session

Syntax **shutdown**

Notes Always use this command to perform an orderly shut down before removing power from the switch.

When the shutdown is complete, the Heartbeat LED is extinguished.

Test Command

Tests ports using internal (SerDes level), external (transceiver), and online loopback tests. Internal and external tests require that the port be placed in diagnostic mode. Refer to the "Set Command" on page A-59 for information about changing the port administrative state. While the test is running, the remaining ports on the switch remain fully operational.

Authority Admin session

Syntax **test**

port [port_number] [test_type]
cancel
status

Keywords **port [port_number]** ***[test_type]***

Tests the port given by [port_number] using the test given by [test_type]. If you omit [test_type], Internal is used. [test_type] can have the following values:

internal
Tests the SerDes for all port speeds independent of the capabilities of the transceiver. This is the default. The port must be in diagnostics mode to perform this test.

Note: An internal test on a 10-Gbps port verifies that a complete path exists, but does not send a test frame.

external
Tests both the SerDes and transceiver for all port speeds that are supported by the transceiver. The port must be in diagnostics mode to perform this test, and a loopback plug must be installed in the transceiver.

Note: An external test on a 10-Gbps port verifies that a complete path exists, but does not send a test frame.

online
Tests communications between the port and its device node or device loop at the operating port speed. The port being tested must be online and connected to a remote device. The port passes if the test frame that was sent by the ASIC matches the frame that is received. This test does not disrupt communication on the port.

cancel
Cancels the online test in progress.

status
Displays the status of a test in progress, or if there is no test in progress, the status of the test that was executed last.

Examples To run an internal or external port test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. Place the port in Diagnostics mode, enter the following command (*x* = port number) and press the Enter key.

   ```
   set port x state diagnostics
   ```

3. Choose the type of port loopback test to run:

   - To run an internal loopback test, enter the following:

     ```
     test port x internal
     ```

   - To run an external loopback test, enter the following command. A loopback plug must be installed for this test to pass.

     ```
     test port x external
     ```

4. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload.

5. After the test type has been chosen and the command executed, a message on the screen will appear detailing the test results.

6. After the test is run, put the port back into online state by entering the following command (*x* = port number) and pressing the Enter key.

   ```
   set port x state online
   ```

7. To verify port is back online, enter the following command and press the Enter key. The contents of the AdminState field should display be “Online”.

   ```
   show port x
   ```

The online loopback (node-to-node) test requires that port be online and connected to a remote device. To run the online loopback test, do the following:

1. To start an admin session, enter the following command and press the Enter key.

   ```
   admin start
   ```

2. To run the online loopback test, enter the following command and press the Enter key.

   ```
   test port x online
   ```

3. A series of test parameters are displayed on the screen. Press the Enter key to accept each default parameter value, or type a new value for each parameter and press the Enter key. The TestLength parameter is the number of frames sent, the FrameSize (256 byte maximum in some cases) parameter is the number of bytes in each frame, and the DataPattern parameter is the pattern in the payload. Before running the test, make sure that the device attached to the port can handle the test parameters.

   ```
   SANbox Manager (admin) #> test port x online

   A list of attributes with formatting and current values will
   follow. Enter a new value or simply press the ENTER key to
   accept the default value. If you wish to terminate this
   process before reaching the end of the list press 'q' or 'Q'
   and the ENTER key to do so.

     TestLength    (decimal value, 1-4294967295)   [100    ]
     FrameSize     (decimal value, 36-2148)        [256    ]
     DataPattern   (32-bit hex value or 'Default') [Default]
     StopOnError   (True/False)                    [False  ]
     Do you want to start the test? (y/n) [n]
   ```

4. After all parameter values are defined, press the Y key to start the test. After the command executes, a message on the screen will appear detailing the test results.

Uptime Command

Displays the elapsed up time since the switch was last reset and reset method. A hot reset or non-disruptive firmware activation does not reset the elapsed up time reported by this command.

Authority None

Syntax **uptime**

Examples The following is an example of the Uptime command:

```
SANbox Manager #> uptime

  Elapsed up time  : 0 day(s), 2 hour(s), 28 min(s), 44 sec(s)
  Reason last reset: NormalReset
```

User Command

Administers and displays user accounts.

Authority Admin account name and an Admin session. The Accounts and List keywords are available to all account names without an Admin session.

Syntax

user
accounts
add
delete [account_name]
edit
list

Keywords

accounts
Displays all user accounts that exist on the switch. This keyword is available to all account names without an Admin session.

add
Add a user account to the switch. You will be prompted for an account name, a password, authority, and an expiration date.

- A switch can have a maximum of 15 user accounts.
- Account names are limited to 15 characters; passwords must be 8–20 characters.
- Admin authority grants permission to use the Admin command to open an admin session, from which all commands can be entered. Without Admin authority, you are limited to view-only commands.
- The expiration date is expressed in the number of days until the account expires (2000 maximum). The switch will issue an expiration alarm every day for seven days prior to expiration. 0 (zero) specifies that the account has no expiration date.

delete [account_name]
Deletes the account name given by [account_name] from the switch.

edit
Initiates an edit session that prompts you for the account name for which to change the expiration date and authority.

list
Displays the list of users currently logged in and their session numbers. Provides the same function as the Show Users command. This keyword is available to all account names without an Admin session.

Notes Authority level or password changes that you make to an account that is currently logged in do not take effect until that account logs in again.

Examples

The following is an example of the User Accounts command:

```
SANbox Manager (admin) #> user accounts

    Current list of user accounts
  ----------------------------
  images       (admin authority = False, never expires)
  admin        (admin authority = True , never expires)
  chuckca      (admin authority = False, expires in < 50 days)
  gregj        (admin authority = True , expires in < 100 days)
  fred         (admin authority = True , never expires)
```

The following is an example of the User Add command:

```
SANbox Manager (admin) #> user add
    Press 'q' and the ENTER key to abort this command.
account name (1-15 chars)      : user1
account password (8-20 chars)  : *******

please confirm account password: *******

set account expiration in days (0-2000, 0=never): [0] 100

should this account have admin authority? (y/n): [n] y

OK to add user account 'user1' with admin authority
and to expire in 100 days?

Please confirm (y/n): [n] y
```

The following is an example of the User Edit command:

```
SB211.192 (admin) #> user edit

      Press 'q' and the ENTER key to abort this command.

  account name (1-15 chars)      : user1
  set account expiration in days (0-2000, 0=never): [0]
  should this account have admin authority? (y/n): [n]

  OK to modify user account 'user1' with no admin authority
  and to expire in 0 days?

  Please confirm (y/n): [n]
```

The following is an example of the User Delete command:

```
SANbox Manager (admin) #> user del user3

  The user account will be deleted.  Please confirm (y/n): [n] y
```

The following is an example of the User List command:

```
SANbox Manager (admin) #> user list

    User                          Ethernet Addr-Port    Logged in Since
    ----                          ------------------    ---------------
  admin@OB-session1             10.20.68.108-1031     day month date time year
  admin@OB-session2             10.20.68.108-1034     day month date time year
  snmp@OB-session3              Unknown               day month date time year
  snmp@IB-session4              Unknown               day month date time year
  admin@OB-session5             Unknown               day month date time year
```

Whoami Command

Displays the account name, session number, and switch domain ID for the Telnet session.

Authority None

Syntax **whoami**

Examples The following is an example of the Whoami command:

```
SANbox Manager #> whoami

User name       : admin@session2
Switch name     : SANbox Manager
Switch domain ID: 21 (0x15)
```

Zone Command

Manages zones and zone membership on a switch.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page A-133 for information about starting a Zoning Edit session. The List, Members, and Zonesets keywords are available without an Admin session.

Syntax

zone
add [zone] [member_list]
copy [zone_source] [zone_destination]
create [zone]
delete [zone]
list
members [zone]
remove [zone] [member_list]
rename [zone_old [zone_new]
type [zone] *[zone_type]*
zonesets [zone]

Keywords

add [zone] [member_list]
Specifies one or more ports/devices given by [members] to add to the zone named [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. A zone can have a maximum of 2000 members. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

The application verifies that the [members] format is correct, but does not validate that such a member exists.

copy [zone_source] [zone_destination]
Creates a new zone named [zone_destination] and copies the membership into it from the zone given by [zone_source].

create [zone]
Creates a zone with the name given by [zone]. An zone name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 2000 zones.

delete [zone]
Deletes the specified zone given by [zone] from the zoning database. If the zone is a component of the active zone set, the zone will not be removed from the active zone set until the active zone set is deactivated.

list
Displays a list of all zones and the zone sets of which they are components. This keyword does not require an Admin session.

members [zone]
Displays all members of the zone given by [zone]. This keyword does not require an Admin session.

remove [zone] [member_list]
Removes the ports/devices given by [member_list] from the zone given by [zone]. Use a <space> to delimit aliases and ports/devices in [member_list]. [member_list] can have any of the following formats:

- Domain ID and port number pair (Domain ID, Port Number). Domain IDs can be 1–-239; port numbers can be 0–-255.
- 6-character hexadecimal device Fibre Channel address (hex)
- 16-character hexadecimal worldwide port name (WWPN) with the format xx:xx:xx:xx:xx:xx:xx:xx.
- Alias name

rename [zone_old] [zone_new]
Renames the zone given by [zone_old] to the zone given by [zone_new].

type [zone] ***[zone_type]***
Specifies the zone type given by [zone_type] to be assigned to the zone name given by [zone]. If you omit the [zone_type], the system displays the zone type for the zone given by [zone]. [zone_type] can be one of the following:

soft – name server zone

hardACL – Access control list hard zone. This keyword is case sensitive.

zonesets [zone]
Displays all zone sets of which the zone given by [zone] is a component. This keyword does not require an Admin session.

Examples The following is an example of the Zone List command:

```
SANbox Manager #> zone list

  Zone        ZoneSet
  ------------------
  wwn_b0241f
              zone_set_1

  wwn_23bd31
              zone_set_1

  wwn_221416
              zone_set_1

  wwn_2215c3
              zone_set_1

  wwn_0160ed
              zone_set_1

  wwn_c001b0
              zone_set_1

  wwn_401248
              zone_set_1

  wwn_02402f
              zone_set_1

  wwn_22412f
              zone_set_1
```

The following is an example of the Zone Members command:

```
SANbox Manager #> zone members wwn_b0241f

  Current List of Members for Zone: wwn_b0241f
  --------------------------------
  50:06:04:82:bf:d2:18:c2
  50:06:04:82:bf:d2:18:d2
  21:00:00:e0:8b:02:41:2f
```

The following is an example of the Zone Zonesets command:

```
SANbox Manager #> zone zonesets zone1

  Current List of ZoneSets for Zone: zone1
  ---------------------------------
  zone_set_1
```

Zoneset Command

Manages zone sets and component zones across the fabric.

Authority Admin session and a Zoning Edit session. Refer to the "Zoning Command" on page A-133 for information about starting a Zoning Edit session. The Active, List, and Zones keywords are available without an Admin session. You must close the Zoning Edit session before using the Activate and Deactivate keywords.

Syntax

zoneset
activate [zone_set]
active
add [zone_set] [zone_list]
copy [zone_set_source] [zone_set_destination]
create [zone_set]
deactivate
delete [zone_set]
list
remove [zone_set] [zone_list]
rename [zone_set_old] [zone_set_new]
zones [zone_set]

Keywords

activate [zone_set]
Activates the zone set given by [zone_set]. This keyword deactivates the active zone set. Close the Zoning Edit session before using this keyword.

active
Displays the name of the active zone set. This keyword does not require Admin session.

add [zone_set] [zone_list]
Adds a list of zones and aliases given by [zone_list] to the zone set given by [zone_set]. Use a <space> to delimit zone and alias names in [zone_list].

copy [zone_set_source] [zone_set_destination]
Creates a new zone set named [zone_set_destination] and copies into it the zones from the zone set given by [zone_set_source].

create [zone_set]
Creates the zone set with the name given by [zone_set]. A zone set name must begin with a letter and be no longer than 64 characters. Valid characters are 0-9, A-Z, a-z, _, $, ^, and -. The zoning database supports a maximum of 256 zone sets.

deactivate
Deactivates the active zone set. Close the Zoning Edit session before using this keyword.

delete [zone_set]
Deletes the zone set given by [zone_set]. If the specified zone set is active, the command is suspended until the zone set is deactivated.

list
Displays a list of all zone sets. This keyword does not require an Admin session.

remove [zone_set] [zone_list]
Removes a list of zones given by [zone_list] from the zone set given by [zone_set]. Use a <space> to delimit zone names in [zone_list]. If [zone_set] is the active zone set, the zone will not be removed until the zone set has been deactivated.

rename [zone_set_old] [zone_set_new]
Renames the zone set given by [zone_set_old] to the name given by [zone_set_new]. You can rename the active zone set.

zones [zone_set]
Displays all zones that are components of the zone set given by [zone_set]. This keyword does not require an Admin session.

Notes

- A zone set must be active for its definitions to be applied to the fabric.
- Only one zone set can be active at one time.
- A zone can be a component of more than one zone set.

Examples

The following is an example of the Zoneset Active command:

```
SANbox Manager #> zoneset active

  ActiveZoneSet    Bets
  LastActivatedBy  admin@OB-session6
  LastActivatedOn  day month date time year
```

The following is an example of the Zoneset List command:

```
SANbox Manager #> zoneset list

  Current List of ZoneSets
  ------------------------
  alpha
  beta
```

The following is an example of the Zoneset Zones command:

```
SANbox Manager #> zoneset zones ssss

  Current List of Zones for ZoneSet: ssss
  ---------------------------------
  zone1
  zone2
  zone3
```

Zoning Command

Opens a Zoning Edit session in which to create and manage zone sets and zones. Refer to the ”Zone Command” on page A-127 and the ”Zoneset Command” on page A-131.

Authority Admin session except for the Active, History, Limits, and List keywords. The Clear keyword also requires a zoning edit session.

Syntax

zoning
- active
- cancel
- clear
- edit
- history
- limits
- list
- restore
- save

Keywords

active
Displays information for the active zone set including component zones and zone members. This keyword does not require an Admin session.

cancel
Closes the current Zoning Edit session. Any unsaved changes are lost.

clear

Clears all inactive zone sets from the volatile edit copy of the zoning database. This keyword requires a zoning edit session. This keyword does not affect the non-volatile zoning database. However, if you enter the Zoning Clear command followed by the Zoning Save command, the non-volatile zoning database will be cleared from the switch.

Note: The preferred method for clearing the zoning database from the switch is the Reset Zoning command.

edit
Opens a Zoning Edit session.

history
Displays a history of zoning modifications. This keyword does not require an Admin session. History information includes the following:

- Time of the most recent zone set activation or deactivation and the user who performed it
- Time of the most recent modifications to the zoning database and the user who made them.
- Checksum for the zoning database

limits
Displays the number of zone sets, zones, aliases, members per zone, members per alias, and total members in the zoning database. This keyword also displays the switch zoning database limits, excluding the active zone set, which are described in Table A-29. This keyword does not require an Admin session.

Table A-29. Zoning Database Limits

Limit	Description
MaxZoneSets	Maximum number of zone sets (256)
MaxZones	Maximum number of zones (2000)
MaxAliases	Maximum number of aliases (2500)
MaxTotalMembers	Maximum number of zone and alias members (10000) that can be stored in the switch's zoning database.
MaxZonesInZoneSets	Maximum number of zones that are components of zone sets (2000), excluding those in the orphan zone set, that can be stored in the switch's zoning database. Each instance of a zone in a zone set counts toward this maximum.
MaxMembersPerZone	Maximum number of members in a zone (2000)
MaxMembersPerAlias	Maximum number of members in an alias (2000)

list
Lists all zoning definitions. This keyword does not require an Admin session.

restore
Reverts the changes to the zoning database that have been made during the current Zoning Edit session since the last Zoning Save command was entered.

save
Saves changes made during the current Zoning Edit session. The system informs you that the zone set must be activated to implement any changes. This does not apply if you entered the Zoning Clear command during the Zoning Edit session.

Examples

The following is an example of the Zoning Edit command:

```
SANbox Manager #> admin start
SANbox Manager (admin) #> zoning edit
SANbox Manager (admin-zoning) #>
.
.
SANbox Manager (admin-zoning) #> zoning cancel

  Zoning edit mode will be canceled.  Please confirm (y/n): [n]   y

SANbox Manager (admin) #> admin end
```

The following is an example of the Zoning Limits command:

```
SANbox Manager #> zoning limits

  Zoning Attribute     Maximum   Current   [Zoning Name]
  ----------------     -------   -------   -------------
  MaxZoneSets          256       6
  MaxZones             2000      17
  MaxAliases           2500      1
  MaxTotalMembers      10000     166f
  MaxZonesInZoneSets   2000      19
  MaxMembersPerZone    2000
                                 10        D_1_JBOD_1
                                 23        D_1_Photons
                                 9         D_2_JBOD1
                                 16        D_2_NewJBOD_2
                                 5         E1JBOD1
                                 5         E2JBOD2
                                 3         LinkResetZone
                                 3         LinkResetZone2
                                 8         NewJBOD1
                                 8         NewJBOD2
                                 24        Q_1Photon1
                                 8         Q_1_NewJBOD1
                                 13        Q_1_Photon_1
                                 21        Q_2_NewJBOD2
                                 3         ZoneAlias
                                 3         ZoneDomainPort
                                 4         ZoneFCAddr
  MaxMembersPerAlias   2000
                                 2         AliasInAZone
```

The following is an example of the Zoning List command:

```
SANbox Manager #> zoning list
  Active ZoneSet Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:c3
  Configured Zoning Information
  ZoneSet     Zone      ZoneMember
  --------------------------------
  wwn
              wwn_b0241f
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        21:00:00:e0:8b:02:41:2f
              wwn_23bd31
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:23:bd:31
              wwn_221416
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:14:16
              wwn_2215c3
                        50:06:04:82:bf:d2:18:c2
                        50:06:04:82:bf:d2:18:d2
                        10:00:00:00:c9:22:15:
```

Glossary

Access Control List Zone

Access Control List zoning divides the fabric for purposes of controlling discovery and inbound traffic.

Active Zone Set

The zone set that defines the current zoning for the fabric.

Active Firmware

The firmware image on the switch that is in use.

Activity LED

A port LED that indicates when frames are entering or leaving the port.

Administrative State

State that determines the operating state of the port, I/O blade, or switch. The configured administrative state is stored in the switch configuration. The configured administrative state can be temporarily overridden using the command line interface.

Alarm

A message generated by the switch that specifically requests attention. Alarms are generated by several switch processes. Some alarms can be configured.

Alias

A named set of ports or devices. An alias is not a zone, and can not have a zone or another alias as a member.

AL_PA

Arbitrated Loop Physical Address

Arbitrated Loop

A Fibre Channel topology where ports use arbitration to establish a point-to-point circuit.

Arbitrated Loop Physical Address (AL_PA)

A unique one-byte value assigned during loop initialization to each NL_Port on a loop.

ASIC

Application Specific Integrated Circuit

Auto Save

Zoning parameter that determines whether changes to the active zone set that a switch receives from other switches in the fabric will be saved to permanent memory on that switch.

BootP

A type of network server.

Buffer Credit

A measure of port buffer capacity equal to one frame.

Cascade Topology

A fabric in which the switches are connected in series. If you connect the last switch back to the first switch, you create a cascade-with-a-loop topology.

Class 2 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports wit h acknowledgment provided.

Class 3 Service

A service which multiplexes frames at frame boundaries to or from one or more N_Ports without acknowledgment.

Configured Zone Sets

The zone sets stored on a switch excluding the active zone set.

Default Visibility

Zoning parameter that determines the level of communication among ports/devices when there is no active zone set.

Domain ID

User defined number that identifies the switch in the fabric.

Event Log

Log of messages describing events that occur in the fabric.

Expansion Port

E_Port that connects to another FC-SW-2 compliant switch.

Fabric Database

The set of fabrics that have been opened during a SANsurfer Switch Manager session.

Fabric Management Switch

The switch through which the fabric is managed.

Fabric Name

User defined name associated with the file that contains user list data for the fabric.

Fabric Port

An F_Port

Fabric View File

A file containing a set of fabrics that were opened and saved during a previous SANsurfer Switch Manager session.

Fan Fail LED

An LED that indicates that a cooling fan in the switch is operating below standard.

Flash Memory

Memory on the switch that contains the chassis control firmware.

Force PROM Mode

See Maintenance Mode.

Frame

Data unit consisting of a start-of-frame (SOF) delimiter, header, data payload, CRC, and an end-of-frame (EOF) delimiter.

FRU

Field Replaceable Unit

Heartbeat LED

A chassis LED that indicates the status of the internal switch processor and the results of the Power-On Self-Test.

Inactive Firmware

The firmware image on the switch that is not in use.

In-band Management

The ability to manage a switch through another switch over an inter-switch link.

Initiator

The device that initiates a data exchange with a target device.

In-Order-Delivery

A feature that requires that frames be received in the same order in which they were sent.

Input Power LED

A chassis LED that indicates that the switch logic circuitry is receiving proper DC voltages.

Inter-Switch Link

The connection between two switches using E_Ports.

IP

Internet Protocol

LIP

Loop Initialization Primitive sequence

Logged-in LED

A port LED that indicates device login or loop initialization status.

Maintenance Button

Formerly known as the Force PROM button. Momentary button on the switch used to reset the switch or place the switch in maintenance mode.

Maintenance Mode

Formerly known as force PROM mode. Maintenance mode sets the IP address to 10.0.0.1 and provides access to the switch for maintenance purposes.

Management Information Base

A set of guidelines and definitions for SNMP functions.

Management Workstation

PC workstation that manages the fabric through the fabric management switch.

Mesh Topology

A fabric in which each chassis has at least one port directly connected to each other chassis in the fabric.

MIB

Management Information Base

Multistage Topology

A fabric in which two or more edge switches connect to one or more core switches.

NL_Port

Node Loop Port. A Fibre Channel device port that supports arbitrated loop protocol.

N_Port

Node Port. A Fibre Channel device port in a point-to-point or fabric connection.

Pending Firmware

The firmware image that will be activated upon the next switch reset.

POST

Power On Self Test

Power On Self Test (POST)

Diagnostics that the switch chassis performs at start up.

Principal Switch

The switch in the fabric that manages domain ID assignments.

SANsurfer Switch Manager

Switch management application.

SFP

Small Form-Factor Pluggable.

Small Form-Factor Pluggable

A transceiver device, smaller than a GigaBit Interface Converter, that plugs into the Fibre Channel port.

SNMP

Simple Network Management Protocol

Soft Zone

Soft zoning divides the fabric for purposes of controlling discovery. Members of the same soft zone automatically discover and communicate freely with all other members of the same zone.

Target

A storage device that responds to an initiator device.

User Account

An object stored on a switch that consists of an account name, password, authority level, and expiration date.

VCCI

Voluntary Control Council for Interference

World Wide Name (WWN)

A unique 64-bit address assigned to a device by the device manufacturer.

WWN

World Wide Name

Zone

A set of ports or devices grouped together to control the exchange of information.

Zone Set

A set of zones grouped together. The active zone set defines the zoning for a fabric.

Zoning Database

The set of zone sets, zones, and aliases stored on a switch.

Index

A

access control list zone 3-40, 3-56
account name
  display A-123, A-126
  factory A-2
active zone set 3-34, 3-40
Active Zoneset data window 3-34
Admin
  account name A-7
  authority A-7
Admin command A-8
Admin session timeout A-86
administrative state
  configured 4-20, 5-11
  current 4-20, 5-11
  port 5-11, A-80
  switch 4-20, A-60
alarm
  configuration 4-14, A-67
  configuration defaults A-49
  configuration display A-106
  description A-78
  log A-59, A-92
alias
  add members 3-57, A-9
  copy A-9
  create 3-56, A-9
  delete A-9
  delete members A-10
  description 3-40
  display list A-9
  display members A-10
  remove 3-57
  rename A-10
Alias command A-9
Arbitrated Loop Physical Address A-79
archive configuration 4-36
authentication
  device 3-1, A-27
  trap 4-31
  user 3-1
authority A-7
auto save
  default fabric view file 2-16
  graphing options 5-22
  zoning configuration 3-46

B

beacon A-59
binding A-26, A-30
BootP boot method 4-28
broadcast 4-22, A-92
browser 2-2
browser location 2-16, 5-22

C

certificate 3-7, A-19
CHAP authentication A-27
chassis status A-92
checklist 3-8
CIM command A-11
CIMListener command A-12
CIMSubscription command A-14
command syntax A-6
commands A-7
Common Information Model
  configure A-11
  display listener A-92
  display subscription A-92
  listener A-12
  service 4-26, A-84
  subscription A-14
Config command A-16

configuration
  activate A-16
  archive 4-36
  backup A-16
  copy A-16
  delete A-16
  edit A-16
  list A-16
  reset A-45
  restore 4-37, A-17
  save A-17
  wizard 4-18
configured administrative state 4-20
connection
  Secure Socket Layer A-19
  security 3-7, A-83
contact 4-31
CRC error 4-14
Create command A-19
credits 5-14
current administrative state 4-20

D

data window
  active security 3-19
  Active Zoneset 3-34
  Configured Zonesets 4-13
  description 2-24, 2-27, 2-30
  Devices 3-33, 4-8
  port information 5-8
  port statistics 5-5
  switch 4-8
database
  fabric 3-22
  zoning 3-43
date 4-16
Date command A-22
Decode error 4-14
default
  configuration 4-39
  visibility 3-47, 3-50
  zoning 3-48
default fabric view file
  auto save 2-16
  SANsurfer Switch Manager 2-16
defaults
  alarm configuration A-49
  port configuration A-48
  RADIUS configuration A-50
  security configuration A-52
  services configuration A-51
  Simple Network Management Protocol configuration A-50
  switch configuration A-47
  system configuration A-52
  zoning configuration A-49
device
  authentication 3-1
  nickname 3-36
  scan 5-14
  security 3-9
Devices data window 3-33, 4-8
disk space 2-2
distance 5-14
domain ID
  binding A-26, A-30
  description 4-21
  display A-92
  lock 4-21
donor port 5-2, 5-13, A-92
Dynamic Host Configuration Protocol 4-28

E

E_Port isolation 3-58, 4-21
embedded GUI service 4-25
Error Detect Timeout 4-24
event browser
  filter 3-31
  preference 2-17
  sort 3-32

event logging
by component A-75, A-109
by port A-77, A-110
by severity level A-110
display A-109
restore defaults A-77
save settings A-77
settings A-110
severity level 3-30, A-77
start A-77
stop A-77
event severity 3-30
extended credit wizard 5-14
external test 5-16, A-119

F

F_Port 5-2, 5-13
fabric
add 3-22
add a switch 3-25
database 3-22
delete 3-23
discovery interval 2-16
displaying information 3-27
loop port 5-2, 5-13
management 3-1
management workstation 2-2
merge 3-58
port 5-2, 5-13
rediscovery 3-24
security 3-7
services 3-19
status 3-27
tracker 3-20
tree 2-23
zoning 3-38
Fabric Device Management Interface 4-21, A-92
fabric view file 5-21
auto save 5-22
open 2-16, 3-23
password 5-19
save 2-16, 3-24
faceplate display
data window 2-30
description 2-19, 2-28
factory defaults 4-39, A-45
FC-4 descriptor 5-14
FDMI - See Fabric Device Management Interface
Feature command A-23
File Transfer Protocol
example A-38
service 4-26, A-84
firmware
image file 4-42, A-37
install with CLI A-23
install with SANsurfer Switch Manager 4-42
list image files A-37
non-disruptive activation 4-42, A-36
remove image files A-37
retrieve image file A-37
unpack image A-37
version A-98
Firmware Install command A-23
FL_Port 5-2, 5-13

G

gateway address 4-28, A-86
generic port 5-2, 5-13
global graph type 5-26
graph
print 5-26
rescale 5-26
stack performance 5-23
statistics 5-26
type 5-26
graphic window 2-24

group
  add member 3-15, A-26
  copy A-28
  create 3-13, A-28
  display 3-17
  display member 3-17
  edit member attributes 3-16, A-29
  list A-30
  list members A-30
  Management Server A-28
  remove 3-16
  remove member 3-16, A-30
  rename 3-16, A-30
  type A-28, A-30
Group command A-25
GUI management service 4-25

H

hard reset 4-17
Hardreset command A-33
hardware status 4-44
Heartbeat LED 4-44
help 2-18
Help command A-34
History command A-35
host bus adapter A-92
hot reset 4-17
Hotreset command A-36

I

I/O Stream Guard 5-13, A-64
Image command A-37
in-band management
  description 4-22
  enable 3-20
indication service listener A-12
Initial Start Dialog 2-16
Input Power LED 4-44
internal test 5-16, A-119
internet browser 2-2
interoperability 4-23
IP
  address 4-28, A-86
  configuration 4-28
ISL group A-28
ISL monitoring 4-14

L

layout 2-26
legacy address format 4-24
license key 4-41, A-23
link
  delete 3-24
  selecting 2-26
  status 2-25
Link control frame preference routing A-63
Link data window 3-35
link state database A-93
Lip command A-40
listener
  add A-12
  Common Information Model A-92
  create A-12
  delete A-12
log
  archive A-75
  clear A-75
  display A-76, A-110
  event A-75, A-109
  local A-87
  power-on self test A-96
  remote A-87
logged in users A-98
login limit 3-23, A-2
loop port
  bypass A-79
  enable A-79
  fabric 5-2, 5-13
  initialization A-40
loopback test 5-16
loss of signal monitoring 4-14

M

Management Server
  group A-28
  service 4-26, A-84
manufacturer information A-114
mask address A-86
MD5 authentication A-27
media status 5-4
memory
  activity A-93
  workstation 2-2
menu structure 2-20
Multi-Frame Sequence bundling A-63

N

name server
  display A-93
  export 3-36
  zone 3-39
NDCLA - See Non-disruptive code load and activation
network
  configuration reset A-46
  discovery 4-28, A-86
  gateway address A-86
  interfaces A-92
  IP address A-86
  mask A-86
  properties 4-27, 4-30
Network Time Protocol
  client A-87
  description 4-16
  interaction with Date command A-22
  server address A-87
  service 4-26, A-84
nickname
  create 3-36
  delete 3-37
  edit 3-37
  export 3-37
  import 3-38
node-to-node test 5-17
non-disruptive activation A-36
Non-disruptive code load and activation 4-16
NTP - See Network Time Protocol

O

online
  help 2-18
  test 5-17
operating systems 2-2
orphan zone set 3-40

P

page break A-60
Passwd command A-41
password
  change A-41
  default fabric file 5-21
  default fabric view file 2-15
  factory A-2
  switch A-41
  user account 4-5
performance
  graphs 5-23
  tuning A-63
Ping command A-42
polling frequency 5-22

port
  administrative state 5-11, A-80
  buffer credits 5-14
  configuration 5-10, A-61
  configuration defaults A-48
  configuration display A-106
  counters A-79
  displaying information 5-1
  external test A-119
  group A-28
  initialize A-45
  internal test A-119
  loopback test A-119
  mode 5-2
  online test A-119
  operational information A-94
  operational state 5-3
  performance 5-18, A-93, A-112
  performance tuning A-63
  reset 5-15
  selecting 2-29
  speed 5-3, 5-12, A-79
  status 2-28
  symbolic name 5-14
  test 5-16
  type 5-13
  view 2-17, 2-28
Port Information data window 4-12, 5-8
Port Statistics data window 4-12, 5-5
port/device tree 3-44
power on self test log A-96
preferences
  SANsurfer Performance Viewer 5-22
  SANsurfer Switch Manager 2-16
principal switch 4-21
processor 2-2
properties
  network 4-27, 4-30
  port 5-10
Ps command A-43

Q

Quit command A-44

R

RADIUS - See Remote Authentication Dial-In User Service
RADIUS server
  add 3-2
  authentication order 3-6
  configuration A-81
  configuration defaults A-50
  configuration display A-114
  edit configuration 3-5
  remove 3-4
  reset A-45
read community 4-31
refresh 3-27, 4-7
Registered State Change Notification 5-13, A-64
Remote Authentication Dial-In User Service
  server 3-1
remote log
  configuration 4-29
  enable A-87
  host address A-87
reset
  with POST 4-17
  without POST 4-17
Reset command A-45
Resource Allocation Timeout 4-24
restore configuration 4-37
Reverse Address Resolution Protocol 4-28

S

SANsurfer Management Suite
  Linux install 2-6
  Solaris install 2-8
  uninstall 2-14
  Windows install 2-4
SANsurfer Performance Viewer
  arrange graphs 5-24
  customize graphs 5-24
  display graphs 5-23
  exit 5-19
  preferences 5-22
  start 5-19

SANsurfer Switch Manager
default fabric file 2-12
exit 2-12
Linux install 2-3
Mac OS X install 2-4
preferences 2-16, 5-22
Solaris install 2-3
start 2-10
uninstall 2-13, 2-15
user interface 2-19
version 2-18
web applet A-84, A-87
Windows install 2-3
scan device 5-14
secret A-27
Secure Shell
description 3-7
service 4-26, A-83
Secure Socket Layer
certificate A-19
description 3-7
service A-83
switch time A-22
security
certificate 3-7
configuration 3-17, A-64
configuration defaults A-52
configuration display A-106
connection 3-7
consistency checklist 3-8
database A-46
device 3-9
fabric 3-7
Security command A-53
security database
clear 3-16, A-53
display A-54
display history A-54
limits A-54
security edit session
cancel A-53
initiate A-53
revert changes A-54
save changes A-54
security set
activate 3-18, A-57
add member group A-57
copy A-57
create 3-11, A-57
deactivate 3-18, A-57
delete A-58
delete member group A-58
display 3-17, A-58
display active A-53, A-57
display members A-58
remove 3-16
rename 3-16, A-58
Securityset command A-57
SerDes level test 5-16
service listener A-12
services 4-25
services configuration defaults A-51
Set command A-59
Set Config command A-61
Set Log command A-75
Set Port command A-79
Set Setup command A-81
severity levels 3-30
SFP level test 5-16
SHA-1 authentication A-27
Show command A-91
Show Config command A-106
Show Log command A-109
Show Perf command A-112
Show Setup command A-114
Shutdown command A-118
Simple Network Management Protocol
configuration 4-31, A-85
configuration display A-114
defaults A-50
enable 3-20
proxy 4-31
reset A-46
service 4-26, A-84
trap configuration 4-32
SNMP enabled 4-31
soft zone 3-39, 3-56
static boot method 4-28

status icon color 2-23
steering A-96
subnet mask address 4-28
subscription
  create A-14
  delete A-14
  display A-92
support file 4-41, A-19
switch
  add 3-25
  administrative state 4-20, A-60
  advanced properties 4-23
  configuration 4-18, A-64
  configuration defaults A-47
  configuration display A-106
  delete 3-24
  displaying information 4-7
  hard reset 4-17, A-33
  hot reset 4-17
  icons 3-27
  location 4-31
  log A-87
  management service 4-25, A-83
  manufacturer information A-114
  operational information A-97
  paging 4-15
  properties 4-19
  replace 3-26
  reset 4-16, A-122
  reset without POST 4-17, A-46
  restore factory defaults 4-39
  selecting 2-26
  services A-46, A-83, A-114
  stack 4-33
  status 2-25
Switch data window 4-8
symbolic name
  port 5-14
  switch 4-19
syslog 4-29
system configuration
  change A-86
  defaults A-52
  display A-114
System Fault LED 4-44
system services 4-25

T

Telnet
  service 4-26, A-83
  session timeout A-86
Test command A-119
testing ports 5-16
time 4-16, A-22
time zone A-60
timeout
  Admin session A-86
  Telnet session A-86
  values 4-24
tool bar
  standard 2-22
  zoning 3-44
topology display
  arrange icons 2-26
  data windows 2-27
  description 2-19
  usage 2-25
transceiver status 5-4
transmission speed 5-12
trap
  authentication 4-31
  community 4-31
  configuration 4-32
  SNMP version 4-32

U

upgrade 4-41, A-23
Uptime command A-122

user account
  add A-123
  admin A-2
  admin account A-2
  create 4-3
  default 4-2
  delete A-123
  display A-123
  edit A-123
  list A-123
  logged in A-98
  modify 4-6
  password 4-5
  remove 4-4
  security 3-8
User command A-123

V

version 2-18
version snapshot
  compare 3-21
  export 3-21
  save 3-20
Virtual Interface preference routing A-63

W

web applet
  enable A-87
  service 4-25, A-84
Whoami command A-126
wizard
  configuration 4-18
  extended credit 5-14
  zoning 3-42
working
  directory 2-16, 5-22
  status indicator 2-24
workstation requirements 2-2
write community 4-31

Z

zone
  access control list 3-40
  add member port 3-54, A-127
  copy 3-50, A-127
  create 3-53, A-127
  definition 3-39
  delete A-127
  delete member port A-128
  discard inactive 3-47
  list A-128
  list members A-128
  name server 3-39
  remove 3-51
  remove member port 3-55
  rename 3-55, A-128
  soft 3-39
  type 3-56, A-128
Zone command A-127
zone merge
  description 3-58
  failure 3-58
  failure recovery 3-58
zone set
  activate 3-50, A-131
  active 3-34, 3-40, A-133
  add member zone A-131
  copy A-131
  create 3-49, A-131
  deactivate 3-50, A-46, A-131
  definition 3-40
  delete A-131
  delete member zone 3-51, A-132
  discard inactive 3-47
  display A-132
  display active A-131
  display members A-132
  display zones A-128
  management 3-49
  orphan 3-40
  remove 3-51
  rename 3-55, A-132
  tree 3-44

Zoneset command A-131
zoning 4-23
  configuration 3-46, A-68
  configuration defaults A-49
  configuration display A-106
  database 3-41, 3-43, A-46
  default 3-48
  edit A-133
  history A-134
  limits A-134
  list definitions A-134
  remove all 3-48
  revert changes A-134
  save edits A-134
  wizard 3-42
Zoning command A-133
zoning database
  restore 3-47
  save to file 3-47